

5-13-2006

## Development and Analysis of a Model for Assessing Perceived Security Threats and Characteristics of Innovating for Wireless Networks

Mark Bradley Schmidt

Follow this and additional works at: <https://scholarsjunction.msstate.edu/td>

---

### Recommended Citation

Schmidt, Mark Bradley, "Development and Analysis of a Model for Assessing Perceived Security Threats and Characteristics of Innovating for Wireless Networks" (2006). *Theses and Dissertations*. 1380.  
<https://scholarsjunction.msstate.edu/td/1380>

This Dissertation - Open Access is brought to you for free and open access by the Theses and Dissertations at Scholars Junction. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholars Junction. For more information, please contact [scholcomm@msstate.libanswers.com](mailto:scholcomm@msstate.libanswers.com).

DEVELOPMENT AND ANALYSIS OF A MODEL FOR ASSESSING  
PERCEIVED SECURITY THREATS AND CHARACTERISTICS  
OF INNOVATING FOR WIRELESS NETWORKS

By

Mark Bradley Schmidt

A Dissertation  
Submitted to the Faculty of  
Mississippi State University  
in Partial Fulfillment of the Requirements  
for the Degree of Doctor of Philosophy  
in Business Information Systems  
in the College of Business and Industry

Mississippi State, Mississippi

March 2006


Copyright by  
Mark Bradley Schmidt  
2006

DEVELOPMENT AND ANALYSIS OF A MODEL FOR ASSESSING  
PERCEIVED SECURITY THREATS AND CHARACTERISTICS  
OF INNOVATING FOR WIRELESS NETWORKS

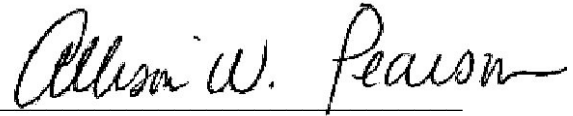
By

Mark Bradley Schmidt

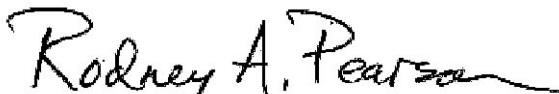
Approved:



Kirk P. Arnett  
Professor of Information Systems  
(Director of Dissertation)




Allison W. Pearson  
Professor of Management  
(Committee Member)



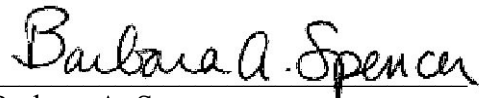
Rodney A. Pearson  
Professor of Information Systems  
(Committee Member)



J. P. Shim  
Professor of Information Systems  
(Committee Member)



Joe H. Sullivan  
Professor of Quantitative Analysis  
(Committee Member)



Barbara A. Spencer  
Professor of Management  
Director of Graduate Studies in the  
College of Business and Industry



Sara M. Freedman  
Dean of the College of Business and Industry

Name: Mark Bradley Schmidt

Date of Degree: March 24, 2006

Institution: Mississippi State University

Major Field: Business Administration (Management and Information Systems)

Major Professor: Dr. Kirk P. Arnett

Title of Study: DEVELOPMENT AND ANALYSIS OF A MODEL FOR  
ASSESSING PERCEIVED SECURITY THREATS AND  
CHARACTERISTICS OF INNOVATING FOR WIRELESS  
NETWORKS

Pages in Study: 233

Candidate for Degree of Doctor of Business Administration

This dissertation employed a two prong approach, whereby the survey and case study methods were used to investigate security issues regarding wireless networks. The survey portion draws together two previously unrelated research streams. Given the recent increased concern for security in the computing milieu, Innovation Diffusion Theory and security factor constructs were merged and synthesized to form a new instrument. This instrument is useful in an effort to understand what role security concerns play in the adoption and diffusion of technology.

In development of the new instrument, 481 usable surveys were collected and analyzed. Factor analysis revealed favorable factor loadings in the data. Further analysis was then conducted utilizing multiple regression analysis. This analysis led

to the discovery that the constructs of Susceptibility and Severity of Threat, Improvement Potential, and Visibility are significant predictors in regard to level of concern when using wireless networks.

Case studies were conducted with a goal to gain a deep knowledge of IT professionals' concerns, attitudes, and best practices toward wireless security. To this end, seven IT professionals were personally interviewed regarding their perceptions and attitudes toward wireless security. In an effort to compare IT professional and end user opinions, 30 IT professionals also completed a paper based survey regarding their perceptions about security. Findings indicate that security professionals are very optimistic for the future of wireless computing. However, that optimism is tempered by a realization that there are a myriad of potential threats that might exploit weakness in wireless security.

To determine differences and similarities between users' perspectives and managers' perspectives regarding wireless network security, the results from the survey and case study were synthesized. Most IT professionals (76.19%) reported that, all factors considered, they prefer to use wired networks as opposed to wireless networks; whereas, substantially fewer (44.86%) of the end user respondents reported that they preferred wired over wireless networks. Overall, results suggest that IT professionals are more concerned about security than are end users. However, a challenge remains to make administrators and users aware of the full effect of security threats present in the wireless computing paradigm.

## DEDICATION

In appreciation of their commitment to my successful completion of the doctoral program, this dissertation is dedicated to my wife Melissa, daughters Taylor and Haylee, and newborn son Spencer. I am very thankful for their love and support.

## ACKNOWLEDGEMENTS

I am extremely appreciative of my parents, Bradley and Cleo Schmidt, for their support of my academic pursuits. More importantly, the work ethic they have instilled in me gave me the courage and ability to pursue my Ph.D.

Any large-scale project, such as a dissertation, can only be as good as the people who are involved in its completion. I was very fortunate to have some extremely talented and dedicated people to provide guidance in the completion of this project.

As an advisor, mentor, and friend, Dr. Kirk P. Arnett played a critical role in my success in the doctoral program. In working with Dr. Arnett over the last few years, I have witnessed first hand a model for professional and personal success that I hope to emulate. I was honored to have worked with one of the most respected professors at Mississippi State University (MSU). His commitment to my ultimate success was and is nothing short of inspirational. He has earned my utmost respect.

For his role in the statistical analysis of the models contained herein, Dr. Joe H. Sullivan, deserves my sincere gratitude. His unparalleled knowledge of statistics and commitment to doctoral student success is a credit to MSU.

Much gratitude goes to Dr. J. P. Shim. Dr. Shim offered much in the way of contribution in the area of wireless communications. As the coordinator of the Business



Information Systems doctoral students, he exhibits a genuine concern for their ultimate success in academia.

For her role in improving my dissertation and expanding my research interests to extend beyond information systems, Dr. Allison W. Pearson deserves many thanks. Her knowledge of methodologies proved very valuable in improving my research.

Dr. Rodney A. Pearson deserves many thanks not only for his work with my dissertation but for his dedication to the classroom as well. By attending his class and observing his approach to classroom success, I have changed my philosophy toward teaching and improved my effectiveness in the classroom.

In addition to my appreciation of my dissertation committee members, I have a great level of appreciation for program of study committee members Dr. Ronald D. Taylor and Dr. Merrill E. Warkentin. Additionally, I would like to commend Dr. Warkentin on his enthusiasm for the profession in general and specifically for his outright passion for research. His commitment to success is a credit to the profession.

Dr. Gary F. Templeton joined the faculty of MSU midway through my program. Based on the short time I have known Dr. Templeton, I have nothing but admiration for his talents and, more importantly, his willingness to play a role in the success of doctoral students. Too numerous to mention are the other faculty and staff that influenced me during my development as a scholar. Nevertheless, their efforts are much appreciated.

Without a doubt, meeting and collaborating with other doctoral students enhanced my success in the doctoral program. Among these fellow doctoral students is my former office partner and very good friend, Dr. Allen C. Johnston. Learning with and from my

peers was a tremendous experience. I feel very fortunate to have had such quality peers to experience the doctoral program with.

Of course, this dissertation would not have been possible without the time and input of Mr. Mike Argo, Mr. Joe Whetstone, Mr. Stein Kristiansen, Mr. David Gresham, Mr. Dean Feller, Mr. Phil Thorson, and Mr. Darrin Printy who were all personally interviewed during my research. Several other IT professionals who took the time to provide their input by completing surveys also made a significant contribution to my research. A final word of appreciation goes to those faculty members who facilitated the end user data collection and to those end users who completed the survey.

## TABLE OF CONTENTS

	Page
DEDICATION .....	ii
ACKNOWLEDGEMENTS .....	iii
LIST OF TABLES .....	ix
LIST OF FIGURES .....	xii
CHAPTER	
I. INTRODUCTION .....	1
Overview .....	1
Innovation Diffusion Theory .....	2
The Case for Wireless Access on Campus .....	3
Problem Statement .....	9
Security Concerns .....	10
Research Questions .....	11
Research Objectives .....	12
Research Methodology in Brief .....	13
Limitations of Study .....	14
Organization of the Dissertation .....	16
II. LITERATURE REVIEW .....	18
Overview .....	18
Wireless Networks as Innovation .....	23
Wireless Access on Campus .....	28
Security .....	30
Wireless Security .....	38
Security Threats Impede Diffusion .....	42
Scale Development for Threats .....	44
Security Risk .....	46
Innovation Diffusion Research in IS .....	48
IDT and Security .....	55
Measuring IDT in IS Research .....	57
Social Systems .....	60
Other Model Considerations .....	61
Academic Research Issues .....	62

CHAPTER	Page
III. RESEARCH METHODOLOGY .....	65
Overview .....	65
Case Study Research .....	66
Strengths and Weaknesses of Case Study Research .....	70
Validity and Reliability Issues of Case Study Research .....	71
The Necessity of a New Instrument .....	73
Sampling Frame .....	74
Hypotheses .....	76
Statistical Techniques .....	88
Factor Analysis .....	88
Logistic Regression .....	88
Sample Size Considerations .....	90
Pilot Case Study .....	91
IV. DATA ANALYSIS .....	94
Overview .....	94
Pilot Case Study Results .....	96
Cases Study Results .....	97
Mangers' Level of Concern .....	100
Mangers' Implementation of Technology .....	103
Security Factors .....	105
Factors of Adoption at the Organizational Level .....	109
Mangers' Perceptions of Security .....	111
Survey Results .....	117
Sample Characteristics .....	120
Factor Analysis .....	123
Logistic Regression .....	139
Evaluation of Research Hypotheses .....	146
Model Construction with MSU-only Data .....	148
Model Construction with WSU-only Data .....	152
Multiple Regression Analysis .....	157
Evaluation of Research Hypotheses in the Final Model .....	161
Synthesis of Case Study and Survey Results .....	166
V. DISCUSSION AND SUMMARY .....	171
Overview .....	171
A Keen Eye on the Future .....	174
Recommendations .....	176
Limitations .....	177

	Page
Directions for Future Research .....	180
Contributions .....	184
Conclusions .....	187
 BIBLIOGRAPHY .....	 192
 APPENDIX	
A. SURVEY INSTRUMENT .....	208
B. STRUCTURED INTERVIEW QUESTIONS .....	215
C. THE ORIGINAL PCI AN THREAT ITEMS .....	225
D. CONSTRUCTS, ITEMS, AND CORRESPONDING QUESTIONS .....	230

## LIST OF TABLES

TABLE	Page
2.1 Common IEEE 802.11 Standards .....	21
2.2 Comparison of Three Popular IEEE 802.11 Standards .....	22
2.3 The Relative Cost of Connectivity .....	25
2.4 The Five Stages of Innovation Diffusion .....	27
2.5 Scale Items Measuring the Constructs of Severity of Threat and Perceived Susceptibility to Threat .....	43
2.6 Confirmatory Factor Analysis Results .....	45
2.7 Number of Items in Each Scale .....	49
2.8 Components of the “Classical Diffusion Model” .....	51
2.9 Constructs of Innovation Diffusion Theory (IDT) .....	58
2.10 Framework for Classification of IDT Research in IS .....	59
3.1 Common Characteristics of Case Research .....	68
4.1 Data Sources for the Case Study .....	98
4.2 Case Study Interview Details .....	99
4.3 Interviewee Responses .....	102
4.4 Interviewee Responses .....	104
4.5 Abbreviated Taxonomy of Threats .....	106
4.6 Security Mechanisms Employed .....	108

TABLE	Page
4.7	Perceived Preparedness ..... 114
4.8	Individual T-Test results ..... 116
4.9	Data Sources ..... 118
4.10	Summary of Missing Data and Action Taken ..... 120
4.11	Selected Demographics of Respondents ..... 121
4.12	Descriptive Statistics ..... 122
4.13	CFA Results ..... 125
4.14	Loadings Presented in the Original Research ..... 128
4.15	EFA Results Rotated Component Matrix ..... 131
4.16	Constructs Identified in Factor Analysis ..... 133
4.17	Construct Reliability ..... 135
4.18	Pearson Correlations ..... 137
4.19	Compressed Dependent Variables Categories and Frequencies ..... 142
4.20	Parameter Estimates of Multinomial Logistic Regression ..... 143
4.21	Classification Matrix for Model with Non, Light, and Heavy Users .. 144
4.22	Binary Dependent Variables Categories and Frequencies ..... 144
4.23	Model for Binary Dependent Variable ..... 145
4.24	Model Prediction Accuracy ..... 146
4.25	Revised Hypotheses ..... 147
4.26	Significance Level of Constructs for MSU Data for Binary Logistic Regression ..... 149

TABLE	Page
4.27 Predicted Results for MSU-only Data Using Binomial Logistic Regression .....	150
4.28 Significance Level of the Constructs for MSU-only Data Multinomial Logistic Regression .....	151
4.29 Predicted Results for MSU-only Data Using Multinomial Logistic Regression .....	152
4.30 Significance Level of the Constructs for WSU-only Data for Binary Logistic Regression .....	153
4.31 Predicted Results for WSU-only Data Using Binomial Logistic Regression .....	154
4.32 Significance Level of the Constructs for WSU Data for Multinomial Logistic Regression .....	155
4.33 Classification Matrix for Multinomial Logistic Regression Using WSU Data .....	156
4.34 Summary of Results .....	157
4.35 ANOVA Table for Model .....	158
4.36 ANOVA Table for Model with Interaction Terms .....	159
4.37 Constructs in the Model .....	160
4.38 Model Summary .....	161
4.39 Revised Hypotheses for the Final Model .....	162
4.40 T-tests for Security Concern .....	167
4.41 Individual t-test Results .....	169
D.1 Constructs, Items, and Corresponding Questions .....	231



## LIST OF FIGURES

Figure		Page
1.1	US College Campuses with Strategic Plans for Wireless Deployment .....	7
1.2	US Colleges Reporting Coverage that Extends to Every Location on Campus .....	7
1.3	Average Coverage Area of Wireless Networks on US College Campuses .....	8
1.4	The two prong approach .....	14
2.1	The Process of Finding a Reasonable Level of Protection .....	32
3.1	Proposed Model of “Propensity to Adopt” in Light of Security (user) .....	83
3.1a	Proposed Model of “Propensity to Adopt” in Light of Security (user) .....	84
3.1b	Proposed Model of “Propensity to Adopt” in Light of Security (manager) .....	85
3.1c	Proposed Model of “Propensity to Adopt” in Light of Security (manager) .....	86
3.2	Flow Diagram of Research .....	87
4.1	The Contingent Innovation Decision .....	109
4.2	Revised Model for IT Professionals .....	117
4.3	Dependent Variable Histogram (Check Account) .....	140

Figure		Page
4.4	Dependent Variable Histogram (Level of Concern) .....	141
4.5	The Contingent Adoption Decision .....	166
5.1	Modified Taxonomy of Threats .....	183

# CHAPTER I

## INTRODUCTION

Chapter one presents an overview of research concerns relative to wireless networks. This overview is followed by sections describing Innovation Diffusion Theory, wireless networks on campus, the problem statement, research objectives, security concerns, research hypotheses in brief, research methodology in brief, limitations of the study, organization of the dissertation, and concludes with a summary of chapter one.

### **Overview**

Local area networks (LANs) are an effective means to share computing resources including data, software, and peripherals (e.g. central processing units (CPUs), disk drives, printers, plotters, and the like). Wireless local area networks (WLANs) are an extension of LANs that allow users, via wireless cards or other handheld devices, to connect to other network resources without a wired connection. WLANs are rapidly emerging and promise new approaches for developing information systems that offer benefits related to flexibility of distribution, lower costs, and increased mobility (see Bleicher, 2000; Deval, Khosravi, Muralidhar, Ahmed, Bakshi, & Yavatkar, 2003).

The emergence of WLANs poses exciting challenges to the research community such as adoption issues, faster time-to-market, quality of wireless information, and security concerns, among others. Of particular interest to this study is to detail security concerns of wireless network managers and to develop a research derived explanation of characteristics of innovating.

### **Innovation Diffusion Theory**

As described initially in (Rogers, 1962), and later in other work by Rogers, (cf. Rogers, 1995), Innovation Diffusion Theory (IDT) has several constructs including: relative advantage, compatibility, complexity, observability, and trialability. IDT research is conducted in several fields including virtually all of the social sciences, education, geography, and business (Mahajan & Peterson, 1985), and IS is no exception in that regard. Arguably the seminal work on IDT in Information Systems (IS) was by Moore and Benbasat. Their model included the original five constructs as identified by Rogers (1962) and established three additional constructs (voluntariness, image, and result demonstrability) (Moore & Benbasat, 1991). Moore and Benbasat's work, which measures Perceived Characteristics of Innovating (PCI) has been described as isolating a robust, reliable, and valid set of constructs that are "key antecedents to technology adoption decisions" (Plouffe, Hulland, & Vandenbosch, 2001, p. 209).

Innovation diffusion research is "perhaps one of the most widely researched and best documented social phenomena" (Mahajan et al., 1985, p. 7). There are thousands of publications in over two dozen distinct academic areas that address IDT (Mahajan et al.,

1985; Rogers, 2003). Further, IDT is a fertile research stream that provides IS researchers with “well developed concepts and a large body of empirical results applicable to the study of technology evaluation, adoption and implementation” (Fichman, 1992, p. 195).

A critical element affecting the diffusion of an innovation at the organizational level is the acceptance of that innovation at the individual level (Moore, 1987). Consistent with this focus, this dissertation will examine the diffusion of innovations from the individual perspective. Fortunately, the PCI instrument is written in such a manner that it can be used, with slight modifications, in most other diffusion studies (Moore et al., 1991).

### **The Case for Wireless Access on Campus**

Wi-Fi (which is a generic term that refers to the IEEE 802.11 standard) is gaining momentum and mainstream acceptance. It was estimated that there were 3,700 commercial WLANs available in the United States in 2002 and it was projected that there would be over 10,000 such access points by the end of 2003 (Shim, Varshney, Dekleva, & Knoerzer, 2003). In terms of providing contiguous coverage for the United States, it is estimated that it would take 7 million hot spots (Shim, Varshney, Dekleva, & Knoerzer, 2006). In the near future, wireless data access appears set for exponential growth as demand shows no sign of abatement (Shim et al., 2006).

Another metric that can be used to assess the growing popularity of WLANs is that of number of users. According to Gartner, there were five million users of WLANs

in North America by the end of 2003 and there will be 30 million by 2007 (Hollis, 2004). In addition to the recent popularity of WLANs in society at large, the college campus has seen a recent dramatic increase in wireless network implementation and usage (Green, 2003).

Wireless access points create a point of differentiation for customers in industries such as hospitality (Schmidt, Johnston, & Arnett, 2004). Further, the presence of wireless access points can create a competitive environment if they are deployed by certain competitors in an industry. For instance, if a particular university in a given market offers wireless access while other universities in that same market do not, the university that has wireless may advertise their relative level of connectivity and capitalize on the fact that they are a “wired” or a connected but “wireless” campus. Wireless networks are in many cases, complementary to existing wired networks. As the level of connectivity is often a factor in the “best colleges and universities” polls, those campuses offering wireless access may have a competitive advantage over those that do not. For instance, the University of Notre Dame asserts they have earned the distinction of making the “America’s 100 Most Wired Colleges” list for the last three years (University of Notre Dame, 2005).

Many colleges are now considering wireless networks to not only provide a point of differentiation but also to reduce the overall costs of providing campus wide connectivity. According to J. Whetstone, Vice President of Computing and Information Technology Services at Winona State University (WSU) wireless offers many benefits to uses on his campus (personal communication, February 9, 2005).

Among the risks of operating at the forefront of wireless adoption on a college campus is that of security. If an organization is not committed to security, it is at risk because there are many potential ways in which unauthorized parties can gain access to the network. Because the data are moved through airwaves, anyone within range can potentially intercept transmissions and therefore gain unauthorized access to another's information. As wireless networks gain acceptance and popularity in the community, students on college campuses want and expect these wireless services in much the same way that hospitality customers seek Wi-Fi in hotels, restaurants, and other hospitality concerns. Another reason for the growth relates to the relative low costs and low level of difficulty in installation and maintenance of WLANs. While some universities deploy wireless in an effort to differentiate themselves, it is more likely that universities are implementing wireless networks as part of a cost leadership strategy.

In contrasting a wireless access point to a wired port in an average office building, J. Whetstone estimates that a wireless access point, which can accommodate several simultaneous users can be installed at a cost of \$500 in a university setting (personal communication, February 9, 2005) while it may cost as much as \$1,000 per wired port (Panko, 2003). Because of the dedicated bandwidth, wired ports can offer more throughput. However, in most cases an access point can effectively provide the necessary bandwidth for users.

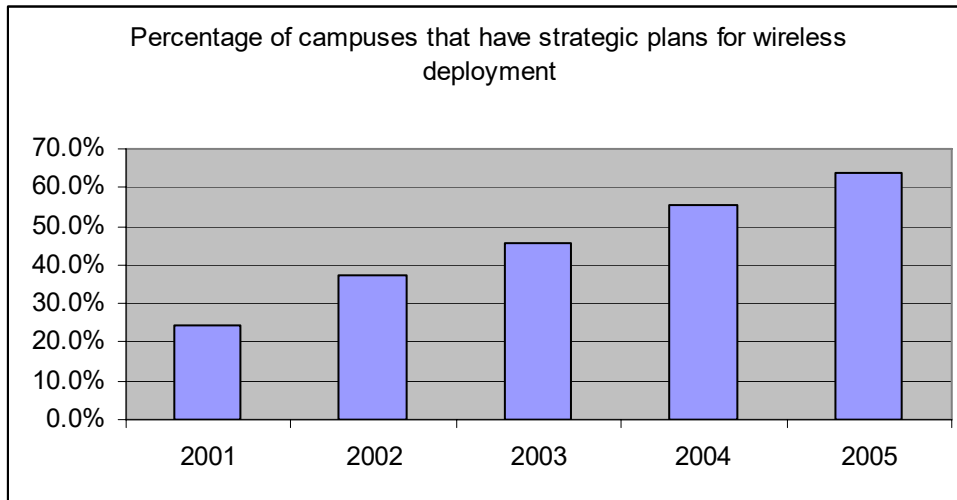
Colleges and universities have been gradually incorporating wireless data access into their infrastructure for the last several years and many campuses now offer ubiquitous access to wireless (New Media Consortium, 2005). According to the 2003

National Survey of Information Technology in US Higher Education, “Wireless is clearly exploding across college campuses, much as it has in the corporate and consumer sectors” (Green, 2003). In fact, according to WSU Network Technician S. Kristiansen, wireless network access is an amenity that numerous students expect to have when they come to campus (personal communication, February 3, 2005). Figure 1.1 depicts the recent dramatic increase in the percentage of college campuses which have strategic plans for their wireless networks. Figure 1.2 demonstrates the increase in the percentage of campuses that indicate they offer campus wide access to the wireless networks. A campus is said to have partial access if they have at least some wireless access points, while a campus with full access will have access on the entire academic portion of campus. Figure 1.3 depicts a nearly three-fold increase in the average percent of campus area that is covered by wireless access points between 2000 and 2003 and further depicts that estimates for 2005 indicate that almost 50% of the campus area is covered. This chart reflects the fact that, on average, the portion of campuses that have wireless access is increasing.

The data used to develop the charts is taken from the 2003 National Survey of Information Technology in US Higher Education, and represents the responses of senior campus officials at 632 public and private colleges and universities in the US (see Green, 2003). The number of wireless networks is definitely on the increase on college campuses, with 55.5% of campus reporting that they were going to deploy wireless networks in 2004 compared with 45.5% in 2004 (Carnevale, 2004). While specific

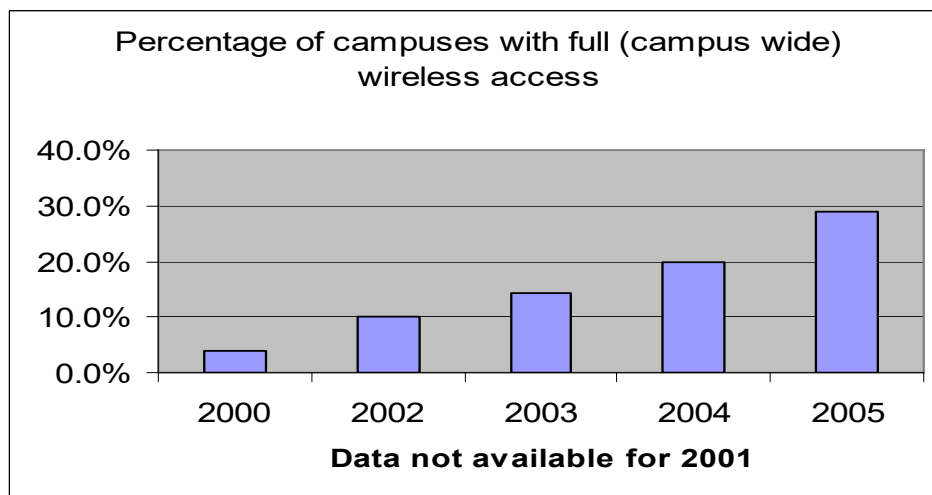


numbers are difficult to obtain, the trend of increasing wireless coverage on college campuses is likely to continue ("Signs of the Times", 2005).



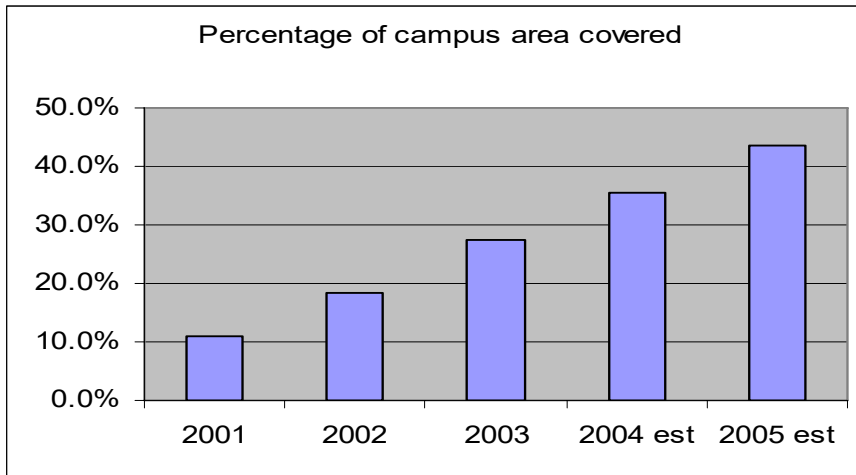
Source: adapted from (Green, 2003, 2005).

Figure 1.1 US College Campuses with Strategic Plans for Wireless Deployment



Source: adapted from (Green, 2003, 2005).

Figure 1.2 US Colleges Reporting Coverage that Extends to Every Location on Campus



Source: adapted from (Green, 2003, 2005).

Figure 1.3 Average Coverage Area of Wireless Networks on US College Campuses

Responding to student and faculty demand, campus administrators may feel pressured to rapidly proceed with the implementation of wireless networks on their campuses. Unfortunately, as many administrators feel pressure to make their campus at least partially wireless, important security concerns may be overlooked. For instance, one university is known to disable the security feature of virtual private networks (VPNs) during home football games to appease the persons who stay on the campus grounds and have difficulty accessing the secured network (M. Argo, personal communication, March 9, 2005). This haphazard approach to security can confound the problem of wireless security. The increasing demand and quick decisions regarding wireless network implementation may lead to significant security problems in the continued operation and use of those networks.

## **Problem Statement**

Two major problems are addressed in this dissertation that relate to the relatively new innovation of WLANs. The first relates to the dearth of research regarding the diffusion of wireless networks at the individual unit of analysis. The second relates to the implementation of wireless networks and the resulting security concerns at the organizational unit of analysis.

One of the major problems addressed is that there is little empirical evidence regarding the important constructs considered by potential users of wireless networks. WLANs have become very popular to many groups of end users (e.g. students, faculty, staff, and visitors) due to the added mobility provided by wireless. Although speculation might suggest cost savings on the provider side and convenience on the consumer side, there are no major studies that address this from a scientific and in-depth perspective. This dissertation will attempt to partially alleviate this dearth by examining student perceptions of WLANs based on a scientific and in-depth perspective. Particular attention will be given to student perceptions of Perceived Characteristics of Innovating and potential security concerns. To operationalize and measure these latent variables, items will be aggregated from previously validated instruments.

The other major problem is that of security or lack thereof in many WLANs (cf. Kahai & Kahai, 2004; Nobel, 2005; Sharma, 2004). A Jupiter Research report entitled “Understanding Corporate WLAN Architecture Choices” indicates that almost 50% of companies consider security concerns as the top impediment to wireless deployment (“WLAN Security: How Big a Problem?” 2004). Given the paramount nature of security

concerns in many industries and organizations, there is a need to increase understanding of security concerns (Computer Security Institute, 2004; Goodhue & Straub, 1989; Whitman, 2003).

Interestingly, there necessarily needs to be a “balance” between security concern issues and ease of use as often times there is an inverse relationship between the two. For instance, if a wireless network does not require the use of virtual private networks (VPNs) and tunneling, both legitimate and non-legitimate users will find it very easy to gain access to the network. Once the access is gained, data including personal information such as passwords can also be obtained by unauthorized parties in the general vicinity of the network. Conversely, if users are required to use VPNs and tunneling to secure access, they may have a difficult time; however, when they are using the network, their data transmissions and stored data are relatively protected from unauthorized parties.

### **Security Concerns**

The theory that security is undervalued by information systems professionals and end users alike has been addressed by researchers for quite some time (Goodhue et al., 1989). Based on her interview with Ian Dobson, Security Director of the Open Group Consortium, Dudman (2004) found one of the most prevalent challenges for IT directors is the rate of business change which then leads to IT infrastructure change. In some cases, the change is “so frantic that it is out of control” (Dudman, 2004, p. 3). Dobson adds that wireless networks are a major source of the security problems, “people are

blasting holes in the firewall to let in legitimate traffic without realizing their potential vulnerability” (Dudman, 2004, p. 3).

Given the significance of security concerns it is then important to increase the understanding of security concerns and threats in both the academic and practitioner communities. University officials and network administrators will be very concerned about security threats in an effort to provide a secure computing environment for students and faculty. The significance of security concerns justifies the need for a new model to address IDT in light of security. This dissertation will attempt to develop such a model.

### **Research Questions**

These research questions will be addressed by a combination of survey data and qualitative data gathered in personal interviews. What impact will voluntariness, relative advantage, compatibility, image, ease of use, result demonstrability, visibility, trialability, severity of threat, and susceptibility to threat have on student intention to use the wireless network? Are there interaction effects between severity of threat and any other variables? Are there interaction effects between susceptibility to threat and any other variables?

What are the differences between user and network manager perceptions? It is believed that network managers will provide a reasonable level of protection to users. Therefore users will not be as concerned with wireless security as they otherwise would need to be in an environment devoid of existing security protection mechanisms.

## Research Objectives

The preceding problems have characterized the need for a greater understanding of security and other critical factors in the adoption and diffusion of wireless networks on college campuses, and to better understand the network manager's thought process with regard to security of those networks. Zmud (1984, p. 737) called for "further research ... such that more precise models for explaining innovation behaviors are developed." Several years later Fichman made a similar call for researchers to continue the task of empirical confirmation of IDT research, further suggesting that a vigorous stream of empirical research could flow from many offshoots of diffusion research (Fichman, 2000).

Mindful of these problems and Zmud's call, the goals of this dissertation are to provide a more precise model to explain critical factors in diffusion of WLANs and to explain how security concerns are balanced with competing factors such as ease of use. An objective of this research is to build upon and extend the prior research examining Perceived Characteristics of Innovating / Innovation Diffusion Theory. To that end, the seminal work on IDT research (Moore et al., 1991), will be extended by synthesizing the Perceived Characteristics of Innovating with perceived severity of and susceptibility to threats (Witte, Cameron, McKeon, & Berkowitz, 1996). Figure 3.1 depicts the model of relationships between the constructs and the dependent variable of "adopting wireless technology."

### **Research Methodology in Brief**

An overview of the methodology to examine the model constructs and to increase understanding of PCI and security concerns is presented here. As depicted in Figure 1.4, this dissertation employs a two-prong approach with somewhat separate but yet interconnected aspirations. Researchers are able to uncover richer and more reliable results when they employ multiple research techniques in the investigation of a phenomenon (Mingers, 2001). The case study method, utilizing face to face and telephone interviews will be employed in an effort to gain an in-depth understanding of the security precautions undertaken by managers of wireless networks. When asked about the increasing trend toward case study and other qualitative research methodologies, Robert Zmud indicated that phenomena under investigation by IS researchers are complex and IS researchers need to strive for diversity and balance while not limiting themselves to the use of a single lens (Lytras, 2005). Consistent with Zmud's opinion, this research will employ a multi methodological approach to investigate two separate perspectives of wireless security.

Additionally, data will be gathered via questionnaire in an effort to understand student perceptions of security concerns in the diffusion of wireless networks. Consistent with the IS research tradition see (Keen, 1980), IDT research draws heavily from other disciplines. Accordingly, there is no single theory that is considered the standard in IDT research, nor is one likely to emerge (Fichman, 2000). However, many IS researchers consider the 1991 work of Moore and Benbasat to be one of the most important innovation theories in IS research.

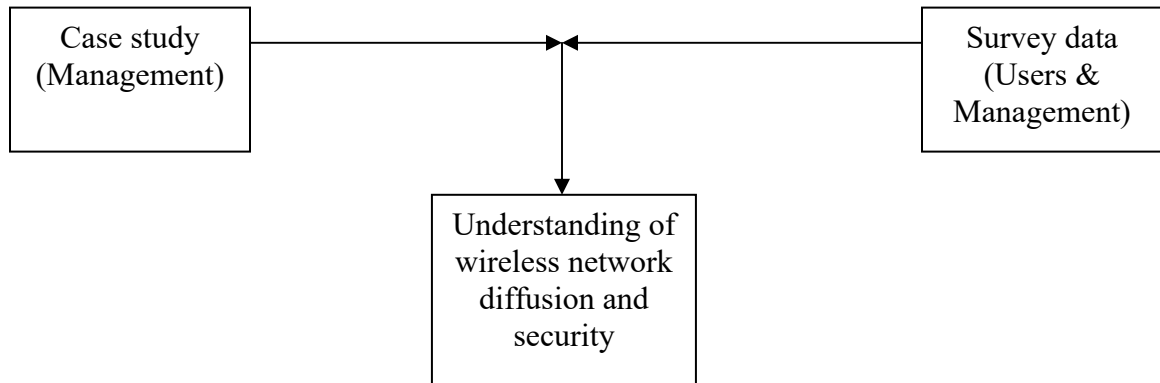


Figure 1.4 The two prong approach

“Diffusion modeling studies represent a tiny fraction of IT innovation research to date” (Fichman, 2000, p. 5). This dissertation then will assist in alleviating this dearth of research and hence contribute to the scientifically grounded understanding of diffusion of information technology.

### **Limitations of the Study**

Although the anticipated sample size of 400 will be sufficient in terms of the research design (Hair Jr., Anderson, Tatham, & Black, 1998), it may be necessary to validate the instrument in other environments before it is appropriate to generalize beyond the university campus environment. As Sitkin and Weingart (1995) suggest, the use of students as research subjects is valid as long as researchers are cognizant of the population to which they can generalize. Students are not the best proxies for decision makers in all situations but as Detmar Straub indicated, researchers can very easily study students and get a general understanding of how people think (personal communication,



April 15, 2005). There are many factors that are suggested to exert an impact on decision behavior under risk. Several of those items include risk preferences, inertia, outcome history, problem framing, top management team homogeneity, social influence, problem domain familiarity, and organizational control systems are but a few gleaned from the management literature (Sitkin & Pablo, 1992).

Additionally, there are many factors that may have additional impact on student perceptions, including a student's previous experience, propensity to embrace new technologies, and perhaps most importantly the issue of the "required" laptop with wireless capabilities. As noted by Network Technician, S. Kristiansen, who is on a campus with a wireless laptop requirement, "we have a much easier time than other schools in terms of providing support" (personal communication, February 3, 2005). When asked for additional information, he expanded on the fact that it is much easier to support a few hardware and software configurations, as is the case with a laptop requirement, rather than having to deal with slightly different configurations from virtually every student, faculty, and staff. This homogeneity plays a pivotal role in affording the helpdesk and other support staff fewer unique configurations to support and thus allowing for a less troublesome environment in which to support end users. However, in the interest of developing a parsimonious model and developing a questionnaire that will not evoke negative reactions regarding its length, these constructs will be reserved for potential future research.

### **Organization of the Dissertation**

This dissertation is divided into five chapters and four appendices. Chapter one presents an overview of the dissertation. Chapter two, entitled “Literature Review,” covers the broad areas of wireless, security, Innovation Diffusion Theory, and case study research. In the first part of the chapter wireless networks as innovations and wireless network use on college campuses are detailed. Chapter two also includes a review of the literature that addresses security issues in information systems in general as well as a review of security issues that specifically pertain to wireless networks. An in-depth review of the work of Moore and Benbasat (1991) is presented as it is critical to the theoretical underpinnings of this research. Chapter two concludes with a discussion of academic research and the case method which includes the seminal work of Yin (2003) and describes how case study research is rich with not only scholarly contribution but with publication potential as well.

Chapter three “Research Methodology” enumerates the research methodology utilized to address the research hypotheses presented in chapter one. The necessity of a new instrument as well as the sampling frame is described. After the hypotheses are developed in detail, the proposed statistical techniques are presented. Specifically, confirmatory factor analysis will be employed to ensure construct validity of the synthesized scales. While the individual scales have been previously validated in published work, the combined scales have yet to be proven and they further require validation in the context of wireless network diffusion. In addition to the quantitative

issues addressed above, chapter three also enumerates details on how the pilot case study was conducted.

Chapter four is entitled “Data Analysis.” This chapter will present the results of the research methodology. Specifically, the results of the factor analysis, summated scale creation, and logistic regression will be presented.

“Discussion and Summary,” is the fifth and final chapter of this dissertation. This chapter presents the results of the study. The overall success of this dissertation and the accomplishment of the goals will be addressed. Chapter five concludes with a summary of the dissertation and its contributions to the scientific and practitioner communities. The bibliography follows chapter five.

Several appendices are also included in this dissertation. Appendix A “Survey Instrument” presents the survey instrument in the form it was given to respondents. Appendix B “Structured Interview Questions” presents the questions asked network managers and other decision makers in regard to their implementation of wireless networks and the security procedures employed. Appendix C “The Original PCI and Threat Items”, includes the short and long instruments as originally proposed by Moore and Benbasat. Appendix D details the constructs, items, and questions.

## CHAPTER II

### LITERATURE REVIEW

Chapter two presents a review of the relevant literature for this dissertation. A brief overview of the chapter reveals that the literature review details four distinct, yet integral, topical areas. The topical areas addressed are that of wireless computing, security issues, innovation diffusion research in information systems, and case research. The next topical area examines security and includes coverage of wireless security, how security threats impede diffusion, and scale development of threats. The third topical area in this chapter relates to IDT research in IS, and includes coverage of IDT and security, measuring IDT in IS research, social systems, and other model considerations. The final topical area addresses case research, with specific coverage given to strengths and weaknesses of case study research and validity and reliability issues of case research. The chapter concludes with a summary of the four topical areas.

#### **Overview**

With the capabilities of 3G to handle both voice and data and potential for 4G to provide true wireless broadband (Shim, 2005), it is possible that traditional WLANs will effectively merge with cellular phone services in the future. In such an environment,

high speed data access would become virtually ubiquitous in nature. However, WLANs are the primary technology under study in this dissertation. As computing and connectivity become more of an integral part of everyday life the wireless network has become more popular (Borisov, Goldberg, & Wagner, 2001). It is clear that the Internet and e-commerce have reshaped the nature of the relationship between customers and businesses and have impacted entire industries (Daniel & Grimshaw, 2002).

It remains to be seen if broadband wireless access will have such an impact. However, in many industries there is evidence that indicates wireless will have a very dramatic impact. In fact, Tom Higgins, president and CEO of Best Western Hotels indicates that, high speed wireless Internet access is the number one amenity requested by almost everyone, particularly businesspeople (Veiga, 2004). Wireless access is by no means a new technology. In fact, wireless access points have been available since the early 1990s. Wireless access points have even been pushed by computer bellwethers such as Gateway and Dell since the late 1990s. According to a 2003 study which included a representative U.S. sample of age 18 and over respondents, 38% of the people are at least somewhat familiar with the technology (Laver, 2003). More recently, a 2004 survey revealed that on average respondents scored a five when asked how familiar they were with Wi-Fi technologies, the scale used was zero to seven with zero on the unfamiliar end of the continuum and seven on the very familiar end of the continuum (Rysavy, 2004).

Wireless network access offers a very convenient and inexpensive mechanism that allows users to share resources such as computers, printers, and access to the Internet

and email. Creating a small wireless network for a home or small office is very simple. Step 1, purchase a wireless access point (WAP), as of early 2005, the cost of a WAP was approximately \$70. Step 2, install the WAP, with the easy to follow directions, this procedure takes you from package to operation in under 30 minutes. Step 3, you can now share files, peripherals, and a single Internet account among all your connected computers without running any network cable.

The preceding steps demonstrate the relative ease and low level of expense that is involved in creating a wireless network. Comparatively, estimates are that to create a wired network, a networker requires \$300 of materials and must complete relatively more steps to interconnect an office with 2 computers and 2 printers (King, 2004). It may take additional time and effort to place the network cable in the walls or other out of the way place. In many cases, a wireless network can be deployed with substantially less time, effort, and money.

Installing wireless access in a larger scale situation can be very cost effective as well. For instance, J. Whetstone estimates that it costs \$2,000 or less to install wireless access to provide coverage to an area equivalent to several classrooms, while it costs 20 – 30 thousand dollars to equip just one classroom with a traditional wired access (personal communication, February 9, 2005). One of the major elements of cost savings relates that one device can provide access to many people via the airwaves. One such device, the “TrueMobile 1170 802.11 b/g Wireless Access Point” can provide connectivity to as many as 250 simultaneous users. The cost of this device is \$389 (Dell Inc., 2005). Moreover, in historical buildings it may be problematic or not feasible to retrofit the

walls with the infrastructure necessary for a wired network. Additionally, the timely manner in which wireless networks can be deployed allows for the creation of ad-hoc networks for emergency services teams, mobile consultants, and other mobile users.

The last few years have been witness to many changes in terms of wireless capabilities. Table 2.1 details several of the common IEEE 802.11 standards.

Table 2.1  
Common IEEE 802.11 Standards

IEEE Standard	Data Rate	Frequency	Comments
802.11a	54 Mbps	5 GHz	The 5 GHz frequency has less interference
802.11b – also known as Wi-Fi	11 Mbps	2.4 GHz	Compatible with 802.11g
802.11g	54 Mbps	2.4 GHz	Compatible with 802.11b
802.11h	N/A	5 GHz	European standard
802.11i	N/A	Describes encryption between 802.11a and 802.11b	Defines new encryption protocols including Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES)
802.11n	108 Mbps +	10 – 20 MHz	Standards are expected to be complete by 2006

There are many choices available in terms of the technology for the access point. However, many implementations seem to utilize 802.11b, 802.11a, or 802.11g. Table 2.2, adapted from (Cisco Systems Inc, 2005), presents a comparison of the aforementioned IEEE standards.

Table 2.2

## Comparison of Three IEEE 802.11 Standards

Relative Advantages of 802.11a / b / g			
IEEE Standard	802.11b	802.11a	802.11g
Popularity	<u>BEST</u> Readily available everywhere.	<u>GOOD</u> New technology.	<u>BETTER</u> New technology with rapid growth expected.
Speed	Up to 11Mbps.	Up to 54Mbps.	Up to 54Mbps.
Relative cost	Inexpensive.	Relatively more expensive.	Relatively inexpensive.
Frequency	2.4 GHz Crowded band – potential interference with cordless phones, microwave ovens, and other devices.	5 GHz Un-crowded band.	2.4 GHz Crowded band – potential interference with cordless phones, microwave ovens, and other devices.
Range	Good range – Typically 100-150 feet depending on building construction and layout.	Shorter range – Typically 25-75 feet indoors.	Good range – Typically 100-150 feet depending on building construction and layout.
Public access.	The number of public hotspots is growing particularly in hotels, airports, restaurants, college campuses, and other public areas.	Limited.	Compatible with current 802.11b hotspots (at the 802.11b rate of 11Mbps) many 802.11b hotspots will be converted to 802.11g.
Compatibility.	Widest adoption.	Incompatible with 802.11b or 802.11g.	Interoperates with 802.11b networks (at 11 Mbps). Incompatible with 802.11a.

Source: adapted from (Cisco Systems Inc, 2005).



## Wireless Networks as Innovation

Innovation, communication channels, time, and social systems are very important factors through the diffusion process (Rogers & Shoemaker, 1971). The last portion of the 20<sup>th</sup> century is typically characterized by many advances in information technology. In fact, many refer to this time period as the information age while others posit that this time period can just as appropriately be termed the “innovation age” (Fichman, 2000). An innovation can be thought of as “an idea, practice, or object perceived as new by an individual.” Additionally, “It matters little, so far as human behavior is concerned, whether or not an idea is ‘objectively’ new as measured by the lapse of time since its first use or discovery” (Rogers et al., 1971, p. 19).

“The nice thing about standards is that there are so many of them to choose from” noted famous computer scientist and mathematician Grace Murray Hopper (Malaga, 2005, p. 119). The advent of wireless network technologies in general and in particular the development of IEEE 802.11 standards is very innovative in that they allow the deployment of wireless local area networks (WLANs).

WLANs offer several advantages which roughly fall into the categories of access and deployment. The advantages of WLANs, in terms of access, center on the concept of mobility. With the deployment of a wireless network, users need not be concerned about being physically connected to an RJ-45 outlet, rather they are allowed to move freely within the range of the wireless access points (WAPs). Typically users must remain within a few hundred feet of an access point. However, the actual range is very dependent on the infrastructure of the building (i.e. nature of the walls, ceilings, and

floors; number of floors, etc) (Dean, 2003). This mobile access to the network has led to the term corridor warrior. Microsoft refers to corridor warriors as persons who require access to electronic information even when they are away from their desks (Microsoft, 2004). This mobility, appreciated in homes, businesses, and college campuses, provides a high level of convenience to users as they move from location to location. These benefits offered by WLANs may even provide a university with a “most wired” or “most unwired” distinction and hence a point of differentiation with those universities that do not offer wireless access.

WLANs offer several benefits to those charged with the deployment of a network. The forefront of these benefits relates to the ease and relative low cost for which the infrastructure can be installed, thus providing the opportunity of a position of cost leadership. According to J. Whetstone, a wireless access point, which can provide connectivity to several simultaneous users, can be installed at a cost of \$500 (personal communication, February 9, 2005). Table 2.3 compares the cost per user to a university in providing connectivity in a wired and wireless manner. These figures represent the cost of the wireless hardware and its installation and they do not reflect other costs such as the cost of the computers that will be used to access the network, maintenance, and the like. The numbers in table 2.3 are based on estimates provided by J. Whetstone (personal communication, February 9, 2005) and (Dell Inc., 2005).

It should be noted however, that the wired network provides a dedicated connection and throughput potential whereas a wireless network shares bandwidth among connected users. Considering the cost of wiring a standard wall jack in the average

existing office building is \$1,000 (Panko, 2003), the cost savings of the WLAN can be substantial. According to Gartner, the total cost of ownership (TCO) comparison between wired and wireless networks is very difficult to make. However, Gartner estimates that the TCO for a wireless network is 15% lower than the TCO of a wired network (Blackwell, 2002). Additionally, it may be problematic to run wire for a LAN in some buildings such as historical sites and in buildings with certain construction. The ease at which a wireless network can be deployed allows for the timely creation of ad-hoc networks for emergency services teams and mobile consultants.

Table 2.3

## The Relative Cost of Connectivity

	Wired (Dedicated throughput)	Wireless (Shared throughput)
Cost per classroom	\$30,000	\$1,000
Number of students	50	50
Cost per student	\$600.00	\$20.00
Throughput	Typically a theoretical maximum of 100Mbps (with Cat 5 cable)	Typically a theoretical maximum of 54Mbps (shared by up to 250 stations or 120 stations when encrypted)

Source: J. Whetstone, personal communication, February 9, 2005 and (Dell Inc., 2005).

A communication channel is “the means by which the message gets from the source to the receiver” (Rogers et al., 1971, p. 24). Wireless technologies are

communication channels themselves in that they allow for somewhat ubiquitous access to connectivity and the propagation of messages from source to the receiver. Given the high speed at which information travels on the Internet and over other networks, WLANs provide a capability to act as their own channel of communication.

Time is a very important component of diffusion research.

The time dimension is involved:

- (1) in the innovation-decision process by which an individual passes from first knowledge of the innovation through its adoption or rejection,
- (2) in the innovativeness of the individual, that is, the relative earliness-lateness with which an individual adopts an innovation when compared with other members of his social system, and
- (3) in the innovation's rate of adoption in a social system, usually measured as the number of members of the system that adopt the innovation in a given time period (Rogers et al., 1971, p. 24-25).

In a study regarding online services diffusion, later adopters were found to discontinue use of innovations at a greater rate than others who adopted at an earlier stage (Parthasarathy & Bhattacharjee, 1998).

Durrington, Repman, and Valente (2000) report that Ryan and Gross (1943) found four stages of innovation. Rogers includes the fifth stage of "confirmation." Table 2.4 summarizes the five stages as presented in (Rogers, 1995).

Table 2.4

## The Five Stages of Innovation Diffusion

Steps in the innovation diffusion process:	Description
Knowledge	Occurs when an individual (or other decision-making unit) learns of the innovation's existence and gains some understanding of how it functions.
Persuasion	Occurs when an individual (or other decision-making unit) forms a favorable or unfavorable attitude toward the innovation.
Decision	Occurs when an individual (or other decision-making unit) engages in activities that lead to a choice to adopt or reject the innovation.
Implementation	Occurs when an individual (or other decision-making unit) puts an innovation into use.
Confirmation	Occurs when an individual (or other decision-making unit) seeks reinforcement of an innovation-decision that has already been made, but the individual may reverse this previous decision if exposed to conflicting messages about the innovation.

Source: adapted from (Rogers, 1995, p. 20).

The rate at which an innovation diffuses throughout a society, organization, or other unit of adoption can vary tremendously. Rogers posits that effective communication, which can increase the rate of diffusion, is more likely to occur between homophilous rather than heterophilous groups (Rogers, 1995). Homophilous groups are found when members share attributes such as beliefs, education, social status, and the like; while heterophilous groups occur when members are very dissimilar on the aforementioned characteristics. In many cases, the students on a college campus constitute a homophilous group of individuals. The students compose such a group by

the very nature of their presence on campus (i.e. they typically experience a very similar educational process and share certain demographics such as age and previous educational experience).

The adoption of the innovation by high profile individuals, termed “opinion leaders,” tends to increase the likelihood of adoption and perhaps even shortens the time it takes for diffusion (Durrington et al., 2000). Conversely, in the academic environment where technology use is voluntary and faculty take great pride in the principles of independence and democracy, opinion leaders, at least the officially recognized opinion leaders (i.e. dean and department chair) may not have a significant influence on technology use (Lewis, Agarwal, & Sambamurthy, 2003). One plausible explanation for this factor is that faculty, who place a great deal of value on autonomy, view the hierarchical relationship between them and administrators as an “administrative necessity” rather than an actual hierarchy (Lewis et al., 2003).

### **Wireless Access on Campus**

The decision for students to adopt wireless access use on a college campus is necessarily a “contingent innovation-decision” in that the individual can only make the accept or reject decision after a prior innovation decision (Rogers, 1995). Examples of research on contingent innovation-decisions include Fichman and Kemerer’s (1999) work on software such as relational database management, fourth generation languages, and computer aided software engineering (CASE) tools; DeSanctis and Poole’s (1994) work

on group decision support systems (GDSS); and Kraut, Rice, and Fish's (1998) work on telephony and communications technologies.

In many cases when an organization adopts an innovation, individuals have at least some level of autonomy in their level of use of the innovation. Some users will exhibit a high level of use and, in fact, use the innovation in ways that expand the capabilities of the innovation while others will limit their use to the most basic functions (Carlson & Zmud, 1999).

Historically many innovations fail to gain a stronghold in the marketplace. For instance, in 1903 Tarde wrote: "... Given one hundred different innovations conceived at the same time—innovations in the form of words, in mythological ideas, industry processes, etc.—ten will spread abroad while ninety will be forgotten." (Rogers, 1995, p. 40). As an example of the fickle nature of the diffusion of innovations, consider the DOVARK keyboard (Rogers, 2003). Even though the DOVARK keyboard is much more efficient for typists, due to the resistance to change on the part of individuals, this innovation has failed miserably to diffuse. Indeed, innovations have been known to fail at a relatively high rate, finding the characteristics of successful innovations and the characteristics of those who adopt innovations should prove to be valuable to scholars and practitioners alike.

A social system can be thought of as a "collectivity of units which are functionally differentiated and engaged in joint problem solving with respect to a common goal" (Rogers et al., 1971, p. 28). Given the preceding definition, it is quite logical to view a typical university as a social system. Given the nature of the university

social system, WLANs on college campuses may experience a somewhat compressed S-curve within the categories innovators, early adopters, early majority, and laggards.

Although beyond the nature and scope of this dissertation, future research should address the rate at which wireless networks have diffused through various universities.

### **Security**

According to Kevin Mitnick, well-known hacker, the best technology, firewalls, intrusion-detection systems, biometric devices are no match for social engineering (Malaga, 2005). People are typically thought of as the weakest link in information security and provide the biggest opportunity for computer criminals to exploit threats. A threat is a possible infringement of security (Bishop, 2003). A threat is a set of situation that has the potential to cause loss or harm (Pfleeger & Pfleeger, 2003). "Information systems are exposed to various sources of danger or loss which are termed security threats" (Warkentin & Schmidt, 2003, p. 2). Threats to computer security have been taken more seriously in the wake of the 9/11 terrorist attacks. Computer systems in one form or another have a large impact on individuals, businesses, organizations, and governments. Accordingly, there is a need for much research in the area of computer security. Despite the seriousness of the threats there is a lack of experts qualified to address the area of IT security (Furnell, Papadaki, Magklaras, & Alayed, 2001). Indeed, in November 2002, lawmakers approved the Cyber Security Research Act, which provides \$900 million to colleges and universities to create computer security centers, attract graduate students, and fund research ("Security Efforts Still Lacking", 2003).



The paradigm of IT security is indeed changing. Today, security experts must also deal with such groups as casual hackers who have downloaded hacking tools from the Internet, terrorists, and people from anywhere in the world who have an Internet connection and a desire to see what they can hack into (Yourdon, 2002). Many of these “new age” hackers have propelled the relative importance of computer security to new heights. In fact, in the case of shopping online, security concerns were found to be more important than perceived ease of use and perceived usefulness (Salisbury, Pearson, Pearson, & Miller, 2001). A major cost of IT is the loss of individual privacy. The convenience and mobility of IT in general and specifically wireless technologies can create real problems in the area of security (Yourdon, 2002), while at the same time the public has demanded greater protection from privacy threats such as identity theft (Luftman & McLean, 2004). In the early days of computers it was relatively easy to secure access to the climate controlled rooms which housed computers, whereas with today’s miniaturized technology, criminals could very easily walk out of the building with a laptop in their brief case or a USB drive, containing the confidential company data, in their pocket (Yourdon, 2002).

While exact figures are extremely difficult to obtain due to a consistent lack of many organizations’ willingness to disclose breaches (Computer Security Institute, 2003; Hoffer & Straub Jr., 1989), industry estimates are that security breaches occur in 90% of organizations each year and cost \$17 billion (Austin & Darby, 2003). A more recent survey found that in 2004 the total losses for 269 companies was \$141 million (Computer Security Institute, 2004). Because of the cost and prevalence of security breaches there is

a need for additional studies in the area of computer security. Consequently, a focus of this research is to increase the awareness level of academicians and practitioners alike to the relevant factors relating to wireless security on college campuses.

Figure 2.1 describes the situation whereby threats and countermeasures are considered in light of a cost benefit analysis to develop a reasonable level of protection. The cost / benefit portion of the model suggests that for systems with relatively low levels of risk for confidentiality, availability, integrity and accountability, a reasonable level of protection can be achieved without high levels of expenditure.

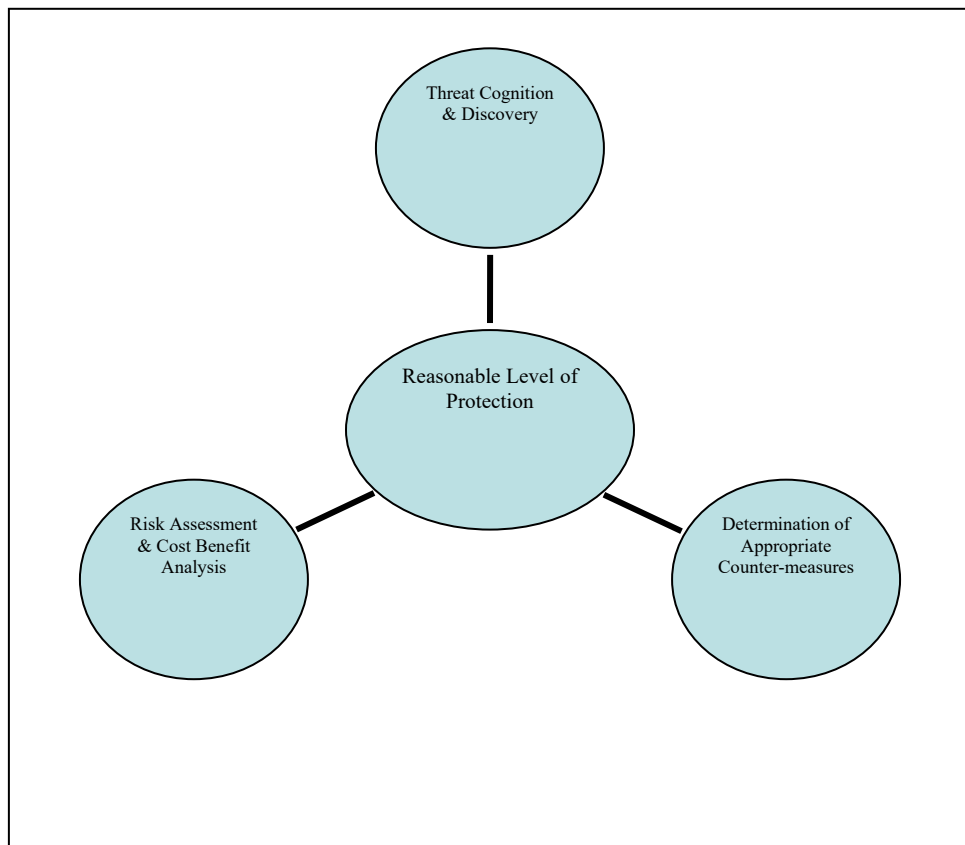


Figure 2.1: The Process of Finding a Reasonable Level of Protection

As Figure 2.1 depicts, threats to that information system need to be considered along with the potential damage that can be caused. This process will vary dramatically depending on the severity of the threat and the vulnerability to that particular threat. For example, the total cost of cleaning up the effects of Code Red was estimated at \$2.6 billion (Austin et al., 2003). In comparison, a defaced web page might be handled by a single person in less than a day. The preceding examples are near the end points on the “cost of cleanup” continuum, and of course, appropriate levels of protection must be implemented based on their location on said continuum.

Considering the level of threat and vulnerability in light of a cost benefit analysis, the next step is to determine the appropriate countermeasures that can be employed to thwart potential threats. Hoffer and Straub (1989) found that security technologies deter computer crime. Examples of typical security technologies used to help deter and detect computer crime include, digital ids, intrusion detection, physical security, encrypted login, firewalls, reusable passwords, anti-virus software, encrypted fields, biometrics, and access control (Computer Security Institute, 2003). The practice of hiring “reformed” hackers as security experts is an option for corporate security offices. However, the practice is not widely endorsed with only 15% of respondents to the eighth annual CSI/FBI Computer Crime and Security Survey indicating a willingness to hire such individuals (Computer Security Institute, 2003).

To operationalize a reasonable level of protection in light of the cost benefit analysis, a particular defense strategy will then be employed. It should be noted that protecting information systems is a never ending cycle. Once a reasonable level of

security is reached, new environmental developments are likely. Consequently, the three steps to a reasonable level of protection are iterative and parallel in nature.

People inside an organization perpetrate most security breaches either by careless or vindictive actions (Austin et al., 2003). Straub and Welke (1998) proposed general deterrence theory and the model of managerial decision making provide solid theoretical underpinnings for the development of an effective security plan. General deterrence theory dictates that people will not participate in criminal activities if the disincentives and sanctions are strong enough (Straub et al., 1998). The model of managerial decision-making gives direction in developing an effective plan to address current issues. Interestingly, many security breaches are not reported to the proper authorities. Worse yet, reporting of such breaches is on the decline (Computer Security Institute, 2004). The main factor in the decision not to report is the fear of negative publicity (Computer Security Institute, 2004). Conversely, in an effort to help deter future computer criminals, it is recommended that more computer abuse be reported to the proper authorities (Straub & Nance, 1990).

The quest to achieve a secure computer system is indeed a difficult one. New developments in hardware and software may serve to increase the likelihood of disasters. When new hardware must be integrated into existing systems (Lally, 2005) hackers and other computer criminals may find a weakness in a newly formed system before they are identified and corrected. Software upgrades (that are poorly tested due to pressure to get the product to market) can increase the likelihood of disaster as they are integrated into existing systems (Lally, 2005). “In spite of the seriousness of systems security risk from

disasters and computer abuse, many organizations are either completely unprotected or insufficiently protected” (Straub et al., 1998, p. 443).

It would seem that organizations would be more vigilant regarding IT security in the wake of such high profile events as the terrorist attacks of September 11, 2001, in which many companies without off site backups lost all of their information assets. Furthermore, recent IT events such as the increase in spyware, high profile viruses and worms such as Code Red, Blaster, and Sobig.F should serve to increase overall awareness of IT security issues. Indeed, the New York Times reports that issues such as disaster preparedness for information technology (IT) have come under increased scrutiny since 9/11 ("Congress Triples Cyber Security Funding", 2003). However, Chris Byrnes, Vice President for security programs at the Meta Group, recently indicated that although companies such as financial institutions are spending 6 – 10% of their IT budgets on security, many companies are not investing enough in IT security. In fact, significant numbers of companies are spending as little as 2% of their IT budget on IT security ("Congress Triples Cyber Security Funding", 2003).

There have been several academic studies that address current issues facing IS professionals. It is interesting to observe the increasing importance of IS security over the last 20 years (see Luftman et al., 2004). Ball and Harris (1982) surveyed the members of the Society of Management Information Systems (SMIS) and found security to be 12<sup>th</sup> most important of 18 concerns facing society members. Dickson, Leitheiser, Nechis, and Wetherbe (1984) surveyed IS professionals and used the Delphi Technique to identify and rank the top IS issues for the 1980s. Their findings put “information

security and control” 14<sup>th</sup> out of 19 identified issues. Two years later, Hartog and Herbert (1986) found IS security to be increasing in importance, at least in the St. Louis area. This study found “data security” to be 6<sup>th</sup> out of 21 issues. As computers and information systems became more integrated in the workplace and as connectivity increased, the area of security became more and more important. K. D. Loch, Carr, and Warkentin (1992) conducted a study that examined the perceptions of senior MIS managers of IS security which reported the relative importance of 12 security threats. One of their findings was that internal threats such as the accidental entry of bad data and the accidental destruction of data by employees are among the most important threats to an information system. The most recent “Key Issues for IT Executives” research finds that security concerns have risen to third on the management concerns list (Luftman et al., 2004). It is interesting to note that at the CIO level, security concerns are number two in the list, perhaps indicating a greater concern for a broader organizational push to ensure the security of information assets.

Threats can be classified on the basis of their origin (inside or outside the company); further, they can be classified on their source (human or nonhuman); and finally they can be classified based on intent (deliberate or unintentional) (see Loch et al., 1992).

- I. Internal
  - a. Human
    - i. Deliberate
    - ii. Unintentional
  - b. Nonhuman

- i. Deliberate
    - ii. Unintentional
- II. External
  - a. Human
    - i. Deliberate
    - ii. Unintentional
  - b. Nonhuman
    - i. Deliberate
    - ii. Unintentional

The following taxonomy was developed using K. D. Loch, Carr, and Warkentin's (1992) work as a starting point. Additional threats were gleaned from, (Bishop, 2003; Kendall & Kendall, 2002; McKeown, 2003; O'Brien, 2001; Oz, 2002; Sanderson & Forcht, 1996; Stair & Reynolds, 2001; Turban, Rainer, & Potter, 2002). These lists were then synthesized to produce the following taxonomy of threats.

- I. Internal
  - a. Human
    - i. Deliberate
      - 1. Unauthorized access by employees
      - 2. Employees intentionally entering improper data
      - 3. Intentional destruction of data by employees
      - 4. Theft of hardware, software, data, or information
    - ii. Unintentional
      - 1. Data entry error by employees
      - 2. Accidental destruction of data by employees
      - 3. Improper media handling
  - b. Nonhuman
    - i. Deliberate
    - ii. Unintentional
      - 1. Weak / ineffective controls
      - 2. Inadequate control over media
      - 3. Poor control of input / output
- II. External
  - a. Human
    - i. Deliberate

1. Hackers / crackers
  2. Access to system by competitors
  3. Social engineering
  4. Dumpster diving
  5. Cyber terrorism
  6. Web site vandalism
  7. Theft of hardware, software, data, or information
- ii. Unintentional
- b. Nonhuman
- i. Deliberate
    1. Viruses / worms / Trojan horses
    2. Denial of service attacks
  - ii. Unintentional
    1. Natural disasters (fires, earthquakes, hurricanes, tornados, floods, storms, severe snow...)
    2. Blackouts / brownouts

### **Wireless Security**

Wireless network security is a topic fecund with research potential. This topic deserves specific attention from at least two reference disciplines. The behavioral sciences can be used to address security implementation from the human factors perspective. For example, Lyytinen (1999) finds that managers' knowledge and perceptions of security have a far reaching impact on the level of security used to protect an asset. However, Straub and Welke (1998) find that despite the seriousness of the nature and scope of the security threats posed by the environment, many organizations are under prepared or completely unprepared to mitigate the threats. Computer science offers much in the way of contribution to the topic of wireless security. Computer science offers the technical background necessary for the provision of security mechanisms such as wired equivalent protocol (WEP) and virtual private networks



(VPN) technologies. Thus, the provision of wireless security needs to be considered from both a human factor and a technical perspective.

“Even though WLANs are widely used, they still lack robust security mechanisms and still provide back-door openings that allow intruders to gain access to them” (Sharma, 2004, p. 118). The nature of this predicament stems from the fact that data is transmitted in wireless networks by radio waves. By their nature, these transmissions are inherently insecure. Whether the infrastructure is composed of copper or fiber, wired networks typically provide a greater level of security. As fiber is extremely difficult to wiretap, it is an appropriate choice when security of the data is critical. Threats to wireless environments exist regardless of industry type, business size, or locale (Attaway, 2003). These threats are significant and potentially harmful if adequate measures of protection are not implemented. The threats can range from minor, such as, the theft of bandwidth to severe as in the case of information theft, modification, or deletion.

Similar to threats against wired network typologies, wireless network security focuses on four essential assurance elements: confidentiality, availability, integrity, and accountability (Vaughn, 2003). Confidentiality refers to the process of protecting information from acquisition and/or exploitation by unintended parties. The confidentiality of data involved in a wireless transmission is maintained through the use of encryption technology. The most prevalent wireless standard in use today, IEEE 802.11b, includes the Wired Equivalent Privacy (WEP) encryption layer to provide data encryption. The primary function of WEP is to prevent eavesdropping and ensure confidentiality of data in transit (Borisov et al., 2001).

Many organizations are currently utilizing IEEE 802.11b as the standard of choice for providing wireless access in a local geographic area (Chen & Nath, 2003).

Unfortunately, WEP only provides a thin layer of protection, as it is easily compromised by numerous hacking techniques (Phifer, 2003). Initially WEP utilized a 40-bit key but now can utilize a 128-bit key. In fact, 128-bit WEP is recommended by Microsoft (Microsoft, 2005). The 128-bit key, although more secure than the 40-bit key, is still not totally secure (Sharma, 2004). Although WEP is better than no protection mechanisms, it is recommended that additional precautions be taken to ensure the security of network traffic (Borisov et al., 2001). Considering the increase concern for security, the future may hold 512-bit or even stronger encryption.

Availability is the process of sustaining the technology in a form that is usable for its intended purposes. IEEE 802.11b is certainly adequate in terms of providing wireless services; however, because of its high-risk status, any guarantee of intended use of the technology is questionable at best. Integrity refers to the reliability of data. In a wireless environment, the integrity of data in transmission from one host to another is easily threatened. A proven method of mitigation is through the use of VPN technologies that allow for the secure transmission of data over wireless media by providing encryption and authentication services. Wireless traffic is isolated to a non-routable, private network where a VPN gateway isolates the routable network (Internet) in a typical VPN. Through the use of VPN client software, a user can be authenticated and be provided an encrypted tunnel for data traffic. Accountability refers to the process by which purveyors of technology are able to hold individuals or parties responsible for their actions. The use of

VPN technology in a wireless environment provides a mechanism by which routed traffic requires an authenticated and encrypted source. This requirement of authentication provides a mechanism to identify those persons responsible for improper activity on a network.

Previous research has established a considerably large set of threats to the confidentiality, integrity, availability, and accountability of wireless network environments (Phifer, 2003; Welch & Lathrop, 2003). As is the case with many emerging technologies, concerns of these threats are often an afterthought. Wireless environment threats can easily translate into risks because of known vulnerabilities in 802.11b. An insertion attack, in which a wireless client is logically “connected” directly into a wireless access point without authorization, is an example of a well-known threat. Another form of insertion attack involves a rogue or unauthorized base station. In this situation, an end-user establishes a personal wireless access point within a wired network without authorization and typically without any security. Additionally, wireless environments are susceptible to wireless traffic analysis, eavesdropping (both active and passive), unauthorized access, man-in-the-middle attacks, replay attacks, denial-of-service attacks, and session hijacking (Welch et al., 2003). On the positive side, the IEEE Task Group I (TG1) is making a serious effort to strengthen the security mechanisms of 802.11 standards, although regrettably, it may take some time to do so (Sharma, 2004).

Advancing technologies, such as wireless networks, that move to make ubiquitous access to information a reality are poised to further threaten our right to privacy. The more data that we disclose and the more that data is made available, the more we run the

risk of what has been termed “minute description” (Mason, 1986). Minute description poses a threat to our privacy when several data sources are effectively merged and integrated to form aggregated information. Ubiquitous access to information can effectively worsen the minute description problem.

Aggregated information can pose a threat to privacy when it is compiled. For example, one institution collects data “A”, which by itself is a minimal threat to privacy; but when synthesized with institution two’s data “B”; and institutions three’s data “C”; and so forth, may prove to be a substantial threat to privacy. Each institution provides a thread of information that when woven together becomes a threat to privacy (Mason, 1986). Mason reports that in *The Cancer Ward: Aleksandr Solzhenitsyn* (1968, p. 221) describes the threat to privacy through aggregated information as follows:

... Every person fills out quite a few forms in his life, and each form contains an uncounted number of questions. The answer of just one person to one question in one form is already a thread linking that person forever with the local center of the dossier department. Each person thus radiates hundreds of such threads, which all together, run into the millions. If these threads were visible, the heavens would be webbed with them, and if they had substance and resilience, the buses, street-cars and the people themselves would no longer be able to move... They are neither visible, nor material, but they were constantly felt by man... Constant awareness of these invisible threads naturally bred respect for the people in charge of that most intricate dossier department. It bolstered their authority.

### **Security Threats Impede Diffusion**

A threat is defined as a danger or harm that exists in the environment whether we are cognizant of it or not. While perceived threat can be defined as cognitions or thought about a particular danger or harm (Witte et al., 1996). Perceived severity of threat and perceived susceptibility to threat are two specific constructs relating to threats. Perceived

susceptibility can be thought of as beliefs about one’s risk of experiencing a threat while perceived severity is defined as beliefs about the importance or magnitude of the threat (Witte et al., 1996). Similar definitions are found in (Witte, 1992). Table 2.5 presents the items used to measure perceived severity of and perceived susceptibility to threat.

Table 2.5  
Scale Items Measuring the Constructs of Severity of Threat and Perceived  
Susceptibility to Threat

Construct	Item
Severity of threat	<ol style="list-style-type: none"> <li>1. I believe that [insert threat here] is severe.</li> <li>2. I believe that [insert threat here] is serious.</li> <li>3. I believe that [insert threat here] is significant.</li> </ol>
Susceptibility to threat	<ol style="list-style-type: none"> <li>1. I am at risk for getting [insert threat here].</li> <li>2. It is likely that I will contract [insert threat here].</li> <li>3. It is possible that I will contract [insert threat here].</li> </ol>

Source: adapted from (Witte et al., 1996).

As applied to wireless network security, severity of threat can be thought of as a “threat” while susceptibility to threat can be thought of as “risk.” In health care, people are not concerned with threats to which they are not vulnerable (e.g. a person who abstains from all risk factors is not susceptible to contracting AIDS). In a similar fashion,

computer users who do not use the wireless network are not vulnerable to security threats regarding the wireless network (i.e. a person with malicious intent using a tool such as Aircrack-ng to sniff packets); therefore, the persons likely perceive their risks to be low or nonexistent.

### **Scale Development for Threats**

In operationalizing the constructs of severity of threat and susceptibility to threat, Witte et al. used items “virtually identical to the operationalizations of these constructs” used in the literature over the last 20 years (Witte et al., 1996, p. 323). To further ensure the validity of the items, 10 independent raters were asked to classify each item into its respective construct category and did so with a success rate of 94%. Fishbein and Ajzen’s (1975) methodology for scale development was utilized in creating the scale (i.e. context and situation sensitive items were developed in an effort to increase accuracy and precision). Perceived susceptibility and perceived severity were averaged to develop an overall index.

In addressing validity, Witte et al. used Cronbach’s alpha. Perceived susceptibility was found to have a relatively high Cronbach’s alpha of .85 while perceived severity has a value of .90. When perceived susceptibility and perceived severity were merged to form an index (perceived threat), Cronbach’s alpha was relatively lower at .54. Table 2.6, adapted from (Witte et al., 1996), demonstrates the factor loadings. In addition, Cronbach’s alpha, when corrected for measurement error, reached a level of .73. (Hair Jr. et al., 1998) indicate that for exploratory research a

Cronbach's alpha of .60 or greater is sufficient. In light of their findings, the separate constructs of perceived severity of threat and perceived susceptibility to threat will be used in this dissertation.

Table 2.6  
Confirmatory Factor Analysis Results

Item / Scale	Severity	Susceptibility
Severity		
Severe	<b>.90</b>	.26
Significant	<b>.79</b>	.26
Serious	<b>.90</b>	.23
Susceptibility		
Likely	.26	<b>.82</b>
At risk	.20	<b>.90</b>
Possible	.27	<b>.81</b>

Source: adapted from (Witte et al., 1996).

This scale was developed in part to “bridge the gap between theory and practice by providing a user friendly scientific tool for practitioners to use in their daily activities” (Witte et al., 1996, p. 339). In a similar fashion then, the addition of the validated scales of severity of threat and susceptibility to threat to the validated scales from the Moore and Benbasat model should provide a valid instrument to determine if security concerns impede the diffusion of innovations.

## Security Risk

A review of the literature reveals that risk can be thought of as an inherent characteristic of a decision when there is a degree of uncertainty in place relating to differing courses of action (Pablo, Sitkin, & Jemison, 1996). Risk to IT can be thought of as “the likelihood that some threat will attack, or exploit, some vulnerability in the system and a calculation of the potential impact resulting from these attacks or exploitations” (Covert & Nielsen, 2005, p. 21). Due to the fact that many organizations are facing increased risks because of an overwhelming increase in the number of threats, it is becoming more critical for security teams to thwart these threats and decrease the organization’s vulnerability to those threats (Drew, 2005).

In an effort to employ appropriate countermeasures to address risk, the first step is to identify the risk (Schmidt, Lyytinen, Keil, & Cule, 2001). Once the risks are identified, they must be classified in such a manner that allows for a successful risk mitigation stratagem (Keil, Cule, Lyytinen, & Schmidt, 1998). Chubb Insurance underwriter, Paul Skinner, warns that risk to IT can take place in many forms and laments that security to guard against such risk is still regarded as a cost rather than an investment (Chordas, 2004). Unfortunately, many companies often repeat the patterns of learning to fail and failing to learn during the systems development life cycle and the systems development process (Lyytinen & Robey, 1999). When companies fail to consider previous experience (either positive or negative) they have exhibited failure to learn and when they consider failure to be just a part of systems development, they are exhibiting



the behavior of learning to fail. Unfortunately, despite the serious nature of security risks there is a dearth of concern and planning when it comes to security in information systems (Straub et al., 1998).

Risk is an important factor in decision making because it affects several factors in decision making including perceptions of a situation, perceptions of alternatives, and choices made (Pablo et al., 1996). There seems to be risks inherent in the large scale adoption of any innovation, for example, in the early 1980s it was a risk for companies to change existing paradigms and provide personal computers to their staff (Keen & Woodman, 1984). In developing a model to evaluate decision risk, Sitkin and Weingart (1995) include the constructs of risk perception and risk propensity, which are thought to be two direct determinants of decision risk as well as mediators of antecedents of characteristics of the decision maker and the problem situation.

Building on the works of Baird & Thomas, 1985; and Bettman, 1973, Sitkin & Weingart (1995) define risk perception as “an individual’s assessment of how risky a situation is in terms of probabilistic estimates of the degree of situational uncertainty, how controllable that uncertainty is and confidence in those estimates. Risk propensity can be thought of as “an individual’s current tendency to take or avoid risks” (Sitkin et al., 1995, p. 1575). In a similar manner, potential users of a wireless network will have a particular risk perception and a particular level of risk propensity which will have an impact on their ultimate decision regarding the use of wireless networks. Sitkin and Weingart (1995) further found that outcome history, which refers to the perception that one’s own decisions were successful or unsuccessful, and problem framing, which refers

to the degree of opportunity or threat that is presented a decision making scenario, affected one's decision making process in the face of risk.

### **Innovation Diffusion Research in IS**

Consistent with much other IS research, innovation diffusion research has a long history as a multi-disciplinary field, with contributors in the fields of sociology, communication, economics, management, information systems, and others (Fichman, 2000). Innovation research in IS primarily focuses on the individual level of analysis (c.f. Moore et al., 1991); whereas diffusion researchers in other fields pay closer attention to a particular social system (Mahajan et al., 1985). A critical component in the diffusion of an innovation is the acceptance of that innovation at the individual level (Moore, 1987). Consequently, this dissertation will study the diffusion of innovations from the individual perspective. IDT affords IS researchers with thoroughly developed concepts as well as many examples of empirical results applicable to the study of technology evaluation, adoption, and implementation (Fichman, 1992).

In addition to the full scale validated and described in Moore and Benbasat (1991) a "short" scale was introduced as well. Both scales include the following eight constructs: voluntariness, relative advantage, compatibility, image, ease of use, result demonstrability, visibility, and trialability. The effort to offer a more parsimonious scale reduces the items from 39 to 25<sup>1</sup>, this in turn allows for a smaller sample size. Table 2.7 describes the number of items for each construct in both the full and short scales (Moore

---

<sup>1</sup> The text of Moore and Benbasat (p. 192) states that there are 38 items when the items listed on pages 216 and 217 total 39.

et al., 1991). It should be noted, however, that depending on the overall purpose of the study smaller sample sizes may be appropriate. For instance, a study that addressed the unidimensionality, validity, and reliability of Moore and Benbasat's relative advantage and compatibility scales was conducted using all 52 of Moore and Benbasat's items with 15 respondents (Miller, Rainer Jr., & Harper, 1997).

Table 2.7

## Number of Items in Each Scale

Items	Number of items suggested for inclusion in the full scale	Number of items that loaded in the full scale	Number of items in the short scale
Voluntariness	4	4	2
Relative advantage	9	8	5
Compatibility	4	4	3
Image	5	4	3
Ease of use	8	6	4
Result demonstrability	4	4	4
Visibility	7	4	2
Trialability	11	5	2
Total items	52	39	25

Source: adapted from (Moore et al., 1991).

The reduced scale has been successfully utilized by researchers (cf. Plouffe et al., 2001). Plouffe et al.'s model was further reduced because some items did not load well on their respective constructs. To compensate, one item each was dropped from "result demonstrability," "visibility," and "trialability" which left three, two, and two items respectively. The Plouffe et al. study, which provides a direct comparison of the

Technology Acceptance Model (TAM) and perceived characteristics of innovating (PCI), found that TAM was able to account for 32.7 percent of the variance in intention to adopt while PCI was able to explain 45 percent of the variance in intention to adopt. PCI then was able to explain 12.3 percent more of the variance than was TAM. Six of seven of PCI's antecedent constructs (relative advantage, compatibility, image, visibility, trialability, and voluntariness) were found to have a significant impact on intention to adopt. The fact that PCI explains more of the variation is a notable finding because adoption at the individual level is a prerequisite for diffusion at the social system level (Moore, 1987). As a result, the PCI characteristics are robust in that they can provide detail as to the propensity to adopt an innovation.

In a study published by Agarwal and Prasad (1997) compatibility, visibility, trialability, and voluntariness all were found to have a significant impact on Internet usage while relative advantage and ease of use were not. A study on adoption of electronic data interchange (EDI) in the financial industry in Singapore found that the slightly modified constructs of PCI were significant in determining adoption behavior (Teo, Tan, & Wei, 1995). The constructs of relative advantage, complexity, observability, operational risks, and strategic risks were found significant in predicting the "present adoption intention" while complexity, observability, trialability, and strategic risks were found to be significant in predicting "future adoption intention."

Innovation Diffusion Theory (IDT) has been applied in a wide range of fields including hybrid corn (Ryan et al., 1943), medical drugs (Coleman, Katz, & Menzel, 1966), new teaching methods (Carlson, 1965), and computer based patient record keeping

in the medical field (Ash, 1997). In many cases the results demonstrate that many innovations diffuse in similar patterns (Brancheau & Wetherbe, 1990). There are several components of diffusion theory. Table 2.8, adapted from (Fichman, 2000), describes those components as presented in (Rogers, 1995).

Table 2.8

## Components of the “Classical Diffusion Model”

Component	Definitions / issues
Diffusion	The manner in which an innovation spreads to the members of a certain social system over time.
Typical diffusion pattern	Diffusion starts slowly with early innovators and takes off as awareness increases then slows as most members of a social system adopt. This leads to an “S” shaped cumulative adoption curve.
Innovation characteristics	Members of a social system perceive levels of relative advantage, compatibility, complexity, trialability, and observability of innovation. These perceptions lead to the ultimate rate of diffusion.
Adoption characteristics	Some members of a social system are more likely to adopt innovations than are other members. Certain characteristics such as education, age, and job tenure are likely to impact one’s propensity to adopt an innovation.
Adoption decision stages	Adoption occurs in stages flowing from knowledge of the innovation and persuasion, decision, implementation and confirmation.
Opinion leaders and change agents	The actions of certain individuals exert a great deal of influence on other potential adopters. This is particularly true when opinion leaders and change agents are homogeneous in comparison to potential adopters.

Source: adapted form (Fichman, 2000).

The Social Science Citation Index (SSCI) was utilized in an effort to identify studies that drew heavily or expanded on Moore and Benbasat's (1991) scale. The SSCI is available in two forms which cover. The first covers January 1993 to December 1994, and January 1996 to December 1999 and the second covers January 2000 to the present. A search of the former produced 61 articles that cite Moore and Benbasat (1991), while a search of the latter returned 149 articles. The search revealed that from 2000 – 2005 there were 149 papers that cited their work.

The lists of 61 and 149 articles were then examined for articles that were published in top IS journals (e.g. MISQ, ISR, and CACM). According to Zmud, the field of MIS has two journals that are invariably considered as "top journals", those two journals are MIS Quarterly and Information Systems Research (Lytras, 2005). Unfortunately, the SSCI does not include works from 1995. To address this lapse in coverage, additional measures were undertaken in an effort to identify important literature published in that year. To that end, EBSCO host was used to specifically target MISQ, ISR, and CACM). The term "innovation diffusion" was entered in the default field's text box and the respective journals were listed in the journal name textbox. This search yielded no additional articles with the terms "innovation diffusion" published in the top IS journals during 1995. The search revealed that MISQ had 13 articles, ISR had 19, and CACM had five articles regarding innovation diffusion.

In addition to the literature identified in the SSCI, a search was conducted in EBSCO host to look for studies in other journals that either utilized or extended Moore and Benbasat's (1991) constructs. This search revealed many articles that cited their

study. A review of the abstracts was then conducted in an effort to isolate articles that heavily relied on their study.

Items from Moore and Benbasat's scale were used in a wide range of additional studies, for instance, technology adoption and continued usage (Karahanna, Straub, & Chervany, 1999); perceived web security and purchase intent (Salisbury et al., 2001); use of Computer Aided Software Engineering (CASE) tools and other software development tools (Fichman et al., 1999; Green & Hevner, 2000); programming language innovations (Agarwal & Prasad, 2000); structured systems development methodologies (Templeton & Byrd, 2003), discontinuance of a previously adopted innovation (Hardgrave, Davis, & Riemenschneider, 2003), and general information technology use by knowledge workers (Lewis et al., 2003).

MIS research is primarily driven by changes in technology rather than managerial issues that are important in the management of technology (Keen, 1980). Keen argues that this "focus" on technology leads to a lack of cumulative tradition as technology changes so rapidly. Fortunately, since Keen's notable work on MIS research, there have been several theories and models that are able to transcend changing technologies. As evidenced by other authors utilizing and leveraging their work, the theory of PCI (see Moore et al., 1991) and its corresponding instrument is one such example. Because of its 10 plus years of use, the instrument developed by Moore and Benbasat, has assisted in addressing the lack of cumulative tradition that Keen referred to in 1980.

It is generally accepted that organizations are growing increasingly dependent on technology for their very survival (Applegate, Austin, & McFarlan, 2003), and

universities are no exception. Even though senior management and other high level decision makers typically make large scale technology adoption decisions, in many cases the ultimate success or failure of the technology (i.e. diffusion) is determined by the individuals who ultimately utilize the technology (Lewis et al., 2003). From a diffusion perspective, IT implementation can be defined as an organizational effort directed toward diffusing suitable information technology with a specific user community (Cooper & Zmud, 1990).

Building on the position of Lewis et al., it follows that decision makers within a university must make the initial decision in regard to wireless network adoption. However, whether the wireless network will be adopted beyond a pilot study is, at least in part, made by students, faculty, and staff who either embrace or reject the technology. So ultimately then in order for wireless networks to diffuse on a college campus, both decision makers at the university level and end users need to embrace the technology.

MIS is an integration of behavioral, technical, and managerial concerns (Keen, 1980). IDT stems from the behavioral sciences, and due to these theoretical underpinnings, investigates the human aspect of technology, specifically that of the rate at which a technological innovation is adopted and used in a given system. Diffusion can be thought of as a specialized type of communication; specifically, diffusion is the process by which innovations are adopted by members of a given social system (Rogers et al., 1971). In IS research an innovation can be thought of as the acceptance and spread of a technology innovation in a particular market or user community (Loch & Huberman, 1999). As defined by Rogers an innovation is:



... an idea, practice or object that is perceived as new by an individual or other unit of adoption. It matters little, so far as human behavior is concerned, whether or not an idea is “objectively” new as measured by the lapse of time since its first use or discovery. The perceived newness of the idea for the individual determines his or her reaction to it. If the idea is new to the individual, it is an innovation. (Rogers, 1983 , p. 11).

From a macro perspective, diffusion of innovations occur as a result of the cumulative decisions of many individuals to adopt (Moore, 1987). These cumulative decisions occur in various social systems. A social system can be fashioned by the students enrolled in a specific course or people living in a particular neighborhood, a business, organization or government agency, or on a larger scale a state or nation (Mahajan et al., 1985).

### **IDT and Security**

Considering the number of attacks is virtually limitless, and the fact that computer security is arguably non-value added, security has been referred to as today’s Y2K in that security threats impose an incredible unknown for information systems (Hayes, 2002).

From administrative and managerial perspectives, innovative technologies, such as wireless networks, are potential security problems. In fact, it is recommended that all potential technology acquisitions should be assessed for their impact on security as well as their increased efficiencies (Dutta & McCrohan, 2002).

According to John Arsneault, director of network operations for Harvard Business School’s IT Group, “In the past, when we talked about implementing systems security or creating policies for restricting access, discussion would be about how this infringed on freedom and put up barriers to collaboration. That attitude has dramatically changed. Today, the schools that have the funds to do it are implementing systems in a very similar

fashion to corporations” Arsneault as quoted in (Shinn, 2005, p. 25). Many universities are starting to take computer security more seriously. Specifically they are looking at security as more of a technical issue and less of a philosophical issue. Consequently, computer security professionals have made tremendous strides over the past thirty years (Vaughn, 2003). During the same time hackers, virus writers, and others with malicious intent have made similar strides with their tools and techniques (Vaughn, 2003). “We’ve made monumental progress in the last couple of years, but there’s always something more coming” Arsneault as quoted in (Shinn, 2005, p. 29).

Computer criminals may have the upper hand due to the fact that security protection is only as strong as its weakest link (Bishop, 2003).

“The attackers only have to discover a single flaw in the new technology to abuse it, whereas the defender has to find all the flaws. That’s actually impossible. Therefore, the defenders have to be able to deploy responses to threats very, very quickly. The vicious circle has moved to Internet speed.” Richard Baskerville as quoted in (Shinn, 2005, p. 27).

Therefore in an effort to protect users and their information assets, the network administrator needs to be acutely aware of the computing environment by not only monitoring internal equipment and logs but also by keeping track of external developments such as new viruses and worms. Indeed awareness is perhaps the first and foremost important step in protecting information assets. This need for awareness and action is a driving force for the case study of wireless network administrators.

### **Measuring IDT in IS Research**

The original five constructs in IDT are relative advantage, compatibility, complexity, observability, and trialability (Rogers, 1962). Table 2.11 provides a summary of those five constructs plus the additional constructs of voluntariness, image, and result demonstrability added by Moore & Benbasat (1991). A validated instrument was published in 1991 that included the original five constructs as identified by Rogers (1962) and included three additional constructs (Moore et al., 1991). Moore and Benbasat's PCI model, has been described as including a robust, reliable, and valid set of constructs that are "key antecedents to technology adoption decisions" (Plouffe et al., 2001, p. 209).

The two additional constructs are image and voluntariness of use. Image can be defined as the extent to which use of an innovation is perceived to enhance an individual's image or status in their social system; while voluntariness of use can be defined as the extent to which the adoption of an innovation is thought to be voluntary or of free will (Moore et al., 1991). The constructs in the PCI model are highly intuitive, reliable, and have considerable explanatory power in regard to predicting an individual's propensity to adopt an innovation (Plouffe et al., 2001). Table 2.9 describes the eight constructs that are included in the instrument. Specific items to be used to operationalize the constructs can be found in appendix D which begins on page 230.

Table 2.9

## Constructs of Innovation Diffusion Theory (IDT)

Construct	Definition
Relative Advantage*	The degree to which an innovation is perceived as being better than its precursor.
Ease of Use* Originally termed complexity by Rogers	The degree to which an innovation is perceived as being difficult to use.
Image	The degree to which use of an innovation is perceived to enhance one's image or status in one's social system.
Visibility* Originally termed observability by Rogers.	The degree to which one observes others in the organization using the innovation.
Compatibility*	The degree to which an innovation is perceived as being consistent with the existing values, needs, and past experiences of potential adopters.
Results Demonstrability	The tangibility of the results of using the innovation, including their observability and communicability.
Voluntariness of Use	The degree to which use of the innovation is perceived as being voluntary, or of free will.
Trialability*	The degree to which an innovation may be experimented with before adoption.
* Denotes an original construct per Rogers (1962).	

Source: adapted from (Venkatesh, Morris, Davis, & Davis, 2003).

Classic diffusion theory is likely to yield conclusive results in the IS field 1) when the context under study matches the original context (e.g. individual adoption of personal technology; 2) when IS researchers extend IDT to include factors specific to IS; or 3) when the technology under study possesses a relatively small cognitive burden for

potential adopters (Fichman, 1992). Table 2.10 depicts Fichman's framework for the classification of IDT research in IS. The most conclusive results are found in quadrant one (Fichman, 1992). Research falling in quadrants two, three, and four often are found to violate the assumptions of IDT. Quadrant two involves a low cognitive burden but includes the organizational level of analysis. Quadrants three and four both require a high level of cognitive burden. To be placed in quadrant one, a study needs to investigate the diffusion of IT with a relatively low cognitive burden and have low levels of interdependencies at the individual level. Under investigation in this dissertation is the diffusion of wireless technology, which arguably enjoys a relatively low cognitive burden and low levels of interdependencies, at the individual level. As a consequence, this research falls into quadrant one, which was found to produce the most successful results.

Table 2.10

## Framework for Classification of IDT Research in IS

<b>Class of Technology</b>	<b>Type 2 (high knowledge burden or high user interdependencies)</b>	III	IV
	<b>Type 1 (low knowledge burden, low interdependencies)</b>	I ( <u>Classic IDT holds true here</u> )	II
		<b>Individual</b>	<b>Organization</b>
		<b>Locus of Adoption</b>	

Source: adapted from (Fichman, 1992).

Moore and Benbasat's model was able to explain more variation than was TAM (see Davis, 1989). This finding suggests that sacrificing parsimony (TAM consists of a subset of the constructs proposed by PCI) is reasonable when a more inclusive set is able to better predict adoption behavior (Plouffe et al., 2001). One of the most important benefits that is realized when the salient characters of adopters are identified occurs when developers are then able to focus their development efforts in an appropriate manner (Moore, 1987).

Despite the fact that both TAM and PCI were found to be highly intuitive, reliable, and have considerable explanatory power, TAM is more parsimonious and, as such, places fewer requirements on respondents and researchers. Conversely, PCI is able to provide a greater sense of richness that is largely missing from TAM (Plouffe et al., 2001). Given these findings, further examination of PCI in other adoption contexts should be high on the priority list for IS researchers (Plouffe et al., 2001).

### **Social Systems**

A very prominent problem in the diffusion of innovations is that individuals are usually quite heterophilous (Rogers, 1995). One could argue that college students would indeed be very heterophilous, at least across a particular campus. Groups have "opinion leaders" and "change agents." The former are persons who are 1) exposed to more external communication than their followers, 2) enjoy higher social status, and 3) are more innovative than the average member; while the latter are persons who are often

professionals with university degrees who attempt to influence others' innovation decisions (Rogers, 1995).

Interestingly, members of a system who are on the leading edge of innovation are very often perceived as “deviant from the social system” (Rogers, 1995, p. 26) and often viewed by the average member of the system as someone with a lower level of credibility than others in the system. Conversely, once a given innovation is in place, knowledgeable innovators who are often referred to as computer gurus, computer mavens, or power users play an instrumental role in the smooth adoption and integration of an innovation (Attewell, 1992).

### **Other Model Considerations**

The IS community as a whole has been eagerly awaiting researchers to actively embrace the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003). However, it should be noted that many researchers including Ray Panko, feel that Innovation Diffusion Theory is passed over in the IS literature as more of a habit toward TAM than the repudiation of Innovation Diffusion Theory (personal communication, August 5, 2005). UTAUT was considered for this dissertation, however, PCI (Moore et al., 1991) appeared to be more appropriate to provide the theoretical underpinnings for this study for several reasons. First, in operationalizing the constructs in UTAUT, only the top four loading items were included for each construct, even if there were additional items that met the typical minimum threshold for factor scores. A potential source of difficulty with such a practice is the components of each

construct can be eliminated, and perhaps diminishing content validity (Venkatesh et al., 2003). By the authors own admission:

“... the measures for UTAUT should be viewed as preliminary and future research should be targeted at more fully developing and validating appropriate scales for each of the constructs with an emphasis on content validity, and then revalidating the model specified herein (or extending it accordingly) with the new measures” (Venkatesh et al., 2003, p. 468).

One of the advantages in the original TAM was the fact that it was a parsimonious model see (Davis, 1989). However, PCI explains 12.3 percent more of the variance than does TAM see (Plouffe et al., 2001). Similarly, the developers of UTAUT, due to the relatively large number of latent variables, had to be cognizant of the number of items in their questionnaires not only for statistical purposes (e.g. degrees of freedom) but also for the convenience of the respondents. Correspondingly then, in an effort to extend a model that is more robust and explains a reasonable proportion of the dependent variable, PCI (Moore et al., 1991) synthesized with severity of and susceptibility to threat (Witte et al., 1996) emerges as a logical choice.

### **Academic Research Issues**

The goal of academic research is to advance knowledge for the benefit of the scientific community (Dennis & Valacich, 2001). All academic research should be evaluated from a scientific and objective perspective. There are three dimensions on which academic research needs to be evaluated. Those three dimensions are generalizability, realism, and precision (McGrath, 1981). Unfortunately, all research is inherently flawed (Dennis et al., 2001). An effective approach to address the flaws in



each method is to use a combination of methods to produce results that are generalizable, realistic, and precise. Currently, the survey method is most frequently used while laboratory and case studies / field studies are also frequently published in the top seven IS journals (Palvia, Mao, Salam, & Soliman, 2003). There is evidence that the case study / field study method is gaining in popularity as the chosen method for publication (Lee & Liebenau, 1997; Palvia, Mao, Midha, Pinjani, & Salam, 2004; Palvia et al., 2003; Trauth, 2001). In addressing concerns about the relative importance of case study research, Benbasat, Goldstein, and Mead (1988), indicate that the case methodology is neither superior to nor inferior to other research methodologies.

A single research method provides researchers a high level of one of McGrath's three dimensions, while satisfying the other dimensions to a lesser degree (Dennis et al., 2001). In field and case study research, the observed level of realism is typically high. However, in field and case study research, the differing situational factors observed in various locations make analysis difficult exhibiting a detrimental effect of precision. However, the level of realism in field and case study research is noted to be very high as participants are in their own environments and not in an artificial situation.

A properly administered survey that seeks input from a randomly selected proportion of a given population typically results in findings that are more generalizable to the environment. Unfortunately, in a survey the levels of realism and precision are often low. Multi-methodological research can compensate for the flaws inherent in single methodological designs. In fact, Nunamaker, Chen, & Purdin (1990 / 1991, p. 89,

p. 89) state that research methodologies are “complementary and that an integrated multi-dimensional and multimethodological approach will generate fruitful IS research results.”

## CHAPTER III

### RESEARCH METHODOLOGY

While the preceding two chapters introduced the research and provided a review of the literature; the purpose of this chapter is to delineate the manner in which the study will be planned, subjects will be selected, and data will be obtained and analyzed. This chapter details the two-prong approach utilized in this dissertation. Specifically, coverage is presented that discusses the reasons for a unique research instrument. The sampling frame is then addressed and the chapter concludes with discussion regarding the hypotheses, statistical techniques, factor analysis, logistic regression, sample size considerations, and the pilot case study.

#### **Overview**

The survey research will be employed in an effort to extend an established theory. Specifically, key constructs and items from PCI / IDT (Moore et al., 1991) and perceived severity of and susceptibility to threats (Witte et al., 1996) will be presented via a survey to students at two universities. Fichman (2000, p. 33) states that “A rich opportunity exists going forward to confirm these promising streams [Innovation Diffusion Theory]

and synthesize them into more complex and realistic models of IT innovation diffusion and assimilation;” it is hoped that the results of this study will be statistically significant and thus extend the original PCI model to become more realistic by including constructs for security.

In addition to survey research, case study research will be utilized in this dissertation. It has been argued that the most important factor in choosing a research methodology is the nature of the phenomena under investigation (Trauth, 2001). To that end, case studies have been used to “uncover subtleties of process and impact related to the use of information technology” (Trauth, 2001, p. 4). In fact, world renowned sociologist Max Weber thinks it “delusional” to describe social phenomena without describing them from a “particular point of view” (Wynn, 2001).

The case study methodology will be employed in this dissertation in an effort to uncover and document the security factors network managers consider before, during, and after the implementation of wireless networks on college campuses. Additionally managers were asked to complete the same questionnaire that users were. It is believed that managers will place different weights on the constructs when compared with users. Specifically, it is likely that managers will place higher weights on security constructs.

### **Case Study Research**

Case study research in MIS has been described as the investigation of an actual information system as it exists in its unaffected, real-world setting (Lee, 1989). Empirical research can be defined as the process of developing and organizing

knowledge uncovered during observation which is then formulated to support insights and generalizations about the phenomena being investigated (Lauer & Asher, 1988). It is very important to gain an in-depth understanding of a situation prior to prescribing a course of action (Lee & Weber, 2004). Case studies are a very effective means to gain a first hand view of a situation and provide a level of detail that is difficult to obtain via other research methods. Qualitative research techniques, such as the case study method, provide researchers the ability to examine textual resources and use other techniques such as personal interviews to gain a deep insight to a particular phenomenon. Qualitative research yields empirical findings that, although they are typically not generalizable, they are in many cases, transferable to situations where similar phenomenon and characteristics are present ("Writing@CSU: Writing Guide", 2004). According to E. Trauth, case study research has seen an increase in exposure and legitimacy, particularly since the MIS Quarterly series of special issues focusing on qualitative research (personal communication, May 24, 2004). Based on a synthesis of the works of Benbasat 1984, Bonoma 1985, Kaplan 1985, Stone 1979, and Yin 1984 case study research is defined as:

A case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organization). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used. (Benbasat, Goldstein, & Mead, 1987, p. 370)

There are several common themes that emanate throughout much literature written on the subject of case research. Table 3.1 provides a synopsis of many such themes and characteristics.

Table 3.1

## Common Characteristics of Case Research

<ol style="list-style-type: none"> <li>1. Phenomenon is examined in a natural setting.</li> <li>2. Data are collected by multiple means.</li> <li>3. One or few entities (person, group, or organization) are examined.</li> <li>4. The complexity of the unit is studied intensively.</li> <li>5. Case studies are more suitable for the exploration, classification, and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration.</li> <li>6. No experimental controls or manipulation are involved.</li> <li>7. The investigator may not specify the set of independent and dependent variables in advance.</li> <li>8. The results derived depend heavily on the integrative powers of the investigator.</li> <li>9. Changes in site selection and data collection methods could take place as the investigator develops new hypotheses.</li> <li>10. Case research is useful in the study of “why” and “how” questions because these deal with operational links to be traced over time rather than with frequency or incidence.</li> <li>11. The focus is on contemporary events.</li> </ol>
---

Source: (Benbasat et al., 1987).

Case study research has commanded respect since at least the early 1980s (Dubé & Paré, 2003). Additionally, research utilizing qualitative research methods, such as case studies, have been consistently published in major journals in which many American IS researchers publish (Trauth, 2001). According to R. Baskerville, IS researchers publishing in high quality journals in Europe (e.g. the European Journal of Information

Systems) have a greater propensity to conduct case study research in an effort to gain insights that may not otherwise be uncovered by other forms of research (personal communication, December 13, 2004).

Following the lead of European and Australian researchers, U.S. IS researchers have demonstrated an increased acceptance of qualitative research since the late 1980's (Lee et al., 1997). According to A. Lee, case research is not always politically accepted as rigorous; however, it is an important part of the scholarly community (personal communication, August 6, 2004). Indeed case research is an effective methodology for conducting IS research and is used frequently in top journals. The editorial policy of a particular journal will have a significant impact on the number and percentage of case articles accepted for publication. An examination of both the European Journal of Information Systems and MIS Quarterly reveals that approximately 25% of the total articles published from 1990 to 1999 are case studies (Dubé et al., 2003).

Benbasat et al. (1987) indicate that case research is a method to capture the knowledge of practitioners and use that knowledge to develop theories they further state that case studies are an effective manner in which to document the experiences of practice. There are three primary reasons that case studies are viable information systems research stratagem (Benbasat et al., 1987).

1. The researches are afforded the ability to generate theories from practice by learning about the state of the art in a natural setting;
2. Researchers are allowed to understand the nature and complexity of the process taking place and hence can answer "how" and "why" questions;

and

3. Case studies are an appropriate technique to investigate a phenomenon that in which there is little established research.

### **Strengths and Weaknesses of Case Study Research**

Case study and other qualitative research methods are receiving attention in the field of IS. Myers describes qualitative research as follows:

“qualitative research methods were developed in the social sciences to enable researchers to study social and cultural phenomena. Examples of qualitative methods are action research, case study research, and ethnography. Qualitative data sources include observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher’s impressions and reactions” (Myers, 2001, p. 5).

Qualitative research is expanding beyond the social sciences. In fact, a recent study found that 15% of the articles in seven major IS journals are case based research during the period from 1990 – 1999 (Dubé et al., 2003).

As with all academic research, there are strengths and there are flaws inherent to case study research. Perhaps the largest strength is that qualitative researchers can obtain a very detailed and rich understanding of the situation under study. However, a downside is that these results may not be generalizable to the environment. Qualitative research is very flexible as the researcher can read the situation and make appropriate changes as the study progresses.

The main weakness of qualitative research is that it is perceived to be a non-scientific approach and introduces bias, not only from the researcher, but the participant as well. Those who partake in qualitative research think it is a very credible academic



endeavor, while those who are more “by the numbers” may view qualitative research as somewhat less than rigorous. Regardless of the school, it seems clear that qualitative research is gaining some popularity in management information system literature (Lee et al., 2004).

### **Validity and Reliability Issues of Case Research**

If research findings are valid, they indeed measure what they intend to. Like other forms of research, qualitative research can vary in its level of validity. It is important to note that, by its nature, qualitative research can produce valid results. The very rich detail in which data is gathered helps to ensure valid results in qualitative research.

If research findings are reliable, different studies should find the same results. If several people seem to say the same thing it is most likely reliable. That said, many people are skeptical of qualitative research as there is much opportunity for the bias of the researchers affecting the results. This is possible because in many cases, the researcher’s own thoughts, opinions, and mind set effect the interpretation of the data.

In order help ensure that academic research advances the scientific community and society in general, the research must be conducted in a rigorous and systematic manner. Addressing validity and reliability issues can help to ensure that the research is conducted in a rigorous and scientific manner. The following sections address validity and reliability issues in the context of case research.

Construct validity can be defined as establishing correct operational measurements for the constructs under investigation (Yin, 2003). It is possible to achieve construct validity in case study research by incorporating multiple sources of evidence, establishing a logical chain of evidence, involving knowledgeable advisors in reviewing the analysis and findings, and defining variables and data values that are potentially unclear (Merhout & Lee, 2004).

Internal validity is “for explanatory studies only, and not for descriptive or exploratory studies” and defines internal validity as “establishing a causal relationship, whereby certain conditions are shown to lead to other conditions, as distinguished from spurious relationships” (Yin, 2003, p. 34). The case study portion of this dissertation will be exploratory in nature; as the goal will be to extend the rich knowledge base regarding security considerations of wireless network implementations in a university environment. This goal will be achieved by conducting person interviews. Consequently, internal validity is not of the utmost importance in this particular study.

External validity is “establishing the domain to which a study’s findings can be generalized” (Yin, 2003, p. 34). In an effort to ensure external validity, the findings can be tested in other locations, a process called replication logic (Yin, 2003). Replication logic will be utilized in this dissertation in that a pilot study will be conducted in addition to two full case studies.

Yin defines reliability as “demonstrating that the operations of a study – such as the data collection procedures can be repeated, with the same results” (Yin, 2003, p. 34). Multiple sources that provide convergent evidence that support conclusions serve to

increase the reliability of findings (Merhout et al., 2004). In an effort to reduce the effect of bias and minimize errors, a detailed research protocol will be followed and detailed records will be maintained during the process.

### **The Necessity of a New Instrument**

In conducting survey research, the researcher can choose to develop a specific scale tailored to the study; alternatively previously validated and published scales can be used with minor modification. Both techniques have advantages and disadvantages. Studies that develop a scale have the advantage of being very specific in that the constructs can be measured in a context sensitive manner, however, the process of scale development can become long and arduous. Using an existing scale, although convenient, may lack the specificity to measure latent variables under study in an optimal manner. In order to leverage the work of other researchers, Straub suggests that researchers “should use previously validated instruments whenever possible, being careful not to make significant alterations in the validated instrument without revalidating instrument content, constructs and reliability” (Straub, 1989, p. 161).

Researchers can contribute to the scientific community by developing a new model to explain a given phenomena. In some cases, researchers contribute to the scientific knowledge base by applying a particular model in a novel manner or with a previously uninvestigated sampling frame. In other cases, researchers extend the knowledge base by developing a new model through the synthesis of existing models and the compilation of a new model. For instance, Hoffer & Alexander (1992) published a

paper entitled “The Diffusion of Database Machines” in which they selected 10 sources of influence that would affect database diffusion. They determined these sources subsequent to “considerable discussion with IT managers and consulting the literature” (Hoffer & Alexander, 1992, p. 13).

In a similar fashion then, this dissertation will synthesize two areas of research in an effort to develop an innovative new model that measures something that has not been measured to date. The two areas of research stem from Innovation Diffusion Theory (IDT), more specifically items are adapted from PCI published by (Moore et al., 1991) and the constructs of severity of and susceptibility to threats specifically adapted from (Witte et al., 1996). Approximately 30 students will be asked to review the draft instrument in an effort to ensure understandability and clarity. The revised instrument will then be given to approximately 400 potential respondents. The findings, validated with confirmatory factor analysis and further developed and tested with logistic regression, will be useful to researchers in the academic and practitioner communities alike in an effort to assist in obtaining more information regarding how security threats impede diffusion.

### **Sampling Frame**

A “contingent innovation-decision” occurs when an individual can only make the accept or reject decision after a prior innovation decision (Rogers, 1995). By its very nature, a college student’s decision to adopt a wireless network is a contingent innovation-decision. In some instances, a new innovation will be adopted at the

organizational level only to be sparsely deployed within that organization; this situation is termed the assimilation gap. Specifically, an assimilation gap is “the difference between the pattern of cumulative acquisitions and cumulative deployments of an innovation across a population of potential adopters” (Fichman et al., 1999, p. 258).

IDT research can be conducted at the organizational level of analysis or the individual level of analysis. Much organizational level diffusion research is conducted in disciplines such as the social sciences, education, geography and other areas (Ash, 1997; Mahajan et al., 1985). Much of this research involves the development of calculus-based models which can then be utilized to approximate the overall rate at which innovations diffuse throughout the particular unit of analysis under investigation (see Mahajan et al., 1985). Most Innovation Diffusion research in Management Information Systems (MIS) focuses on the individual level of analysis (see Moore et al., 1991) and (Fichman, 2000). Consistent with the approach that many other IS researchers have employed; analysis for this dissertation will be at the individual level. This focus on the individual level unit of analysis will provide the opportunity to extend the PCI model (Moore et al., 1991) by including constructs relating severity of susceptibility to threats (Witte et al., 1996).

Given that an assimilation gap exists, diffusion researchers are cautioned that “diffusion modeling can present an illusory picture of the diffusion process -- leading to potentially erroneous judgments about the robustness of the diffusion process already observed, and of the technology’s future prospects” (Fichman et al., 1999, p. 255). Fortunately, as the quantitative portion of this dissertation focuses on the individual as opposed to the organizational level of analysis, a more accurate representation of the

reality of diffusion of wireless networks should emerge. It then follows that these results will address the problems that Fichman & Kemerer (1999) suggest will plague researchers and practitioners if an assimilation gap is present. Specifically, they warned that researchers could draw inaccurate conclusions regarding the theoretical factors that drive diffusion while practitioners may implement an innovation based on the inaccurate belief that adoption is inevitable.

### **Hypotheses**

One of the two major goals of this study is to provide and assess a more precise model to explain critical factors in diffusion. In particular, this study will attempt to extend the PCI model originally developed by Moore & Benbasat (1991) by including two constructs related to security. In operationalizing the constructs, previously validated scales adapted from Witte et al. (1996) will be utilized. The following two general research questions will be considered from the perspective of the user:

1. What are the critical factors that affect diffusion? and
2. Do security threats impede diffusion?

In an effort to answer the very general research questions, several hypotheses emerge. Please reference Figure 3.1, Figure 3.1a, and Figure 3.1b for the research model. These hypotheses are enumerated below; while specific items to be used can be found in appendix C which can be found beginning on page 225.

*Voluntariness* can be thought of as the ability of an individual to make his or her own choice in regard to adoption of an innovation. As defined by Moore & Benbasat

(1991, p. 195) *voluntariness* is “the degree to which use of the innovation is perceived as being voluntary, or of free will.” Agarwal & Prasad (2000, p. 297) state that *voluntariness* affects an adopter’s decision and in an effort to encourage the adoption of an innovation the problem of “... understanding how to influence innovation usage behavior proactively without resorting to coercion” may emerge. Realizing that *voluntariness* may impact the decision to adopt an innovation leads to the first hypothesis:

*H<sub>1</sub>: Voluntariness will have a significant positive effect on user intention to use the wireless network.*

*Relative advantage* is defined as “the degree to which an innovation is perceived as being better than its precursor” (Moore et al., 1991, p. 195). It stands to reason, *ceteris paribus*, that a potential adopter would adopt an innovation if it exhibits a certain level of advantage over the innovation it may replace, and indeed research confirms this (Lee, 2004). *Relative advantage* can be realized in the form of such issues as beneficial effects to time, effort, economic benefits, and comfort levels (Cragg & King, 1993). In the case of a wireless network, many potential users may perceive the *relative advantage* of increased mobility as advantageous to time, effort, and comfort levels. Thus, as hypothesis two suggests, *relative advantage* is likely an important factor in the decision process:

*H<sub>2</sub>: Relative advantage will have a significant positive effect on user intention to use the wireless network.*

*Compatibility* is “the degree to which an innovation is perceived as being consistent with the existing values, needs, and past experiences of potential adopters”

(Moore et al., 1991, p. 195). Recent research by Kaefer & Bendoly (2004), found *compatibility* significant in the diffusion of electronic data interchange (EDI). Hardgrave, Davis, & Riemenschneider (2003), found *compatibility* significant for systems development methodology adoption. Additionally, Parthasarathy & Bhattacharjee (1998) found that a lack of *compatibility* can lead to discontinuance of a previously adopted technology. A potential adopter of an innovation is likely to want that innovation to be compatible with other innovations currently in use, which leads to hypothesis three:

*H<sub>3</sub>: Compatibility will have a significant positive effect on user intention to use the wireless network.*

*Image* is defined as “The degree to which use of an innovation is perceived to enhance one’s image or status in one’s social system” (Moore et al., 1991, p. 195). A delve into education literature finds that image plays a role among peer group attitudes and actions among college students. As an example, Antonio (2004, p. 463), states “the supposition by researchers that interpersonal environments mediate institutional-level peer group effects is strongly supported by this research, and further, the complexity of the findings underscore a need for researchers and administrators to better understand the role of microenvironments in socialization in college.” Antonio’s findings are based on evidence that points to the fact that image is important, if not particularly important, to college students. Specific to this study, it is believed that if it is the “in thing” students will experience a greater likelihood to choose the wireless innovation, as set forth in the following hypothesis:



*H<sub>4</sub>: Image will have a significant positive effect on user intention to use the wireless network.*

*Ease of use*, which was originally termed *complexity* by Rogers, is defined as, “the degree to which an innovation is perceived as being difficult to use” (Moore et al., 1991, p. 195). The responses will be coded in such a manner that a larger number will indicate an easy to use innovation (lacking complexity). There is much significant IS research that indicates that *ease of use* is an important factor in the decision regarding whether or not to adopt an innovation. Among the most notable are several articles that deal with the Technology Acceptance Model (TAM) (see Davis, 1989; Venkatesh & Davis, 2000; Venkatesh et al., 2003). Davis (1989), defines *ease of use* as “the degree to which a person believes that using a particular system would be free of effort” (p. 320). Consistent with the findings published in the TAM studies, it is theorized that if an innovation is easy to use then potential adopters are more likely to become actual adopters as enumerated in hypothesis five:

*H<sub>5</sub>: Ease of use will have a significant positive effect on user intention to use the wireless network.*

*Result demonstrability* is defined as “the tangibility of the results of using the innovation, including their observability and communicability” (Moore et al., 1991, p. 203). Even when innovations are effective, they may fail to diffuse throughout a system if users are not able to attribute gains to the use of the innovation (Venkatesh et al., 2000). *Result demonstrability* has been found to be significant in several important studies including those of (Agarwal et al., 1997; Karahanna et al., 1999; Moore et al., 1991; Venkatesh et al., 2000). *Result demonstrability* was also found to be significant in

the adoption of broadband Internet in Korea (Mariko, Mariko, & Mariko, 2003). If potential adopters are able to observe first hand the results of an innovation, it is theorized that they are more likely to adopt it themselves, as stated in hypothesis six:

*H<sub>6</sub>: Result demonstrability will have a significant positive effect on user intention to use the wireless network.*

*Visibility* is the degree to which one observes others in the organization using the innovation (Moore et al., 1991). As Bandura found in 1977, one can obtain a great deal of information vicariously from observation (Karahanna et al., 1999). As stated in hypothesis seven, if an innovation is seen being used by others it may stimulate others into using the innovation:

*H<sub>7</sub>: Visibility will have a significant positive effect on user intention to use the wireless network.*

*Trialability* can be thought of as “the degree to which an innovation may be experimented with before adoption” (Moore et al., 1991, p. 195). The ability to conduct a risk free trial of an innovation allows for the reduction in uncertainty surrounding an innovation and will serve to increase a potential adopters comfort level and thus increase their propensity to use and diffuse the innovation themselves (Karahanna et al., 1999). For the aforementioned reasons, it stands to reason that if one is able to try an innovation, he or she may be more likely to adopt it, thus the eighth hypothesis:

*H<sub>8</sub>: Trialability will have a significant positive effect on user intention to use the wireless network.*

Perceived threat can be defined as “cognitions or thought about that danger or harm,” while a threat is defined as “a danger or harm that exists in the environment whether we know it or not” (Witte et al., 1996, p. 320). *Perceived severity* can be defined

as “beliefs about the significance or magnitude of the threat,” (Witte et al., 1996, p. 320).

It stands to reason that if one perceives the severity of threat to be high that threats are likely to impede the usage levels of an innovation, thus hypothesis nine:

*H<sub>9a</sub>: Severity of threat will have a significant negative effect on user intention to use the wireless network.*

Perceived *susceptibility* can be defined as “beliefs about one’s risk of experiencing the threat” (Witte et al., 1996, p. 320). Logically if there is threat or danger inherent to a given innovation, a potential adopter is likely to be somewhat reluctant to adopt that innovation, particularly when they perceive a level of susceptibility to that threat, as suggested in hypothesis ten:

*H<sub>9b</sub>: Susceptibility to threat will have a significant negative effect on user intention to use the wireless network.*

Risk perceptions and risk propensity were traditionally thought to exert a direct effect on factors in risk decision making Sitkin & Pablo (1992) propose that such variables actually moderate the other independent variables rather than exert a direct effect. The aforementioned factors lead to hypothesis 10 and 11.

*H<sub>10</sub>: There are interaction effects between perceived severity of threat and any of the other independent variables.*

*H<sub>11</sub>: There are interaction effects between perceived susceptibility of threat and any of the other independent variables.*

In addition to the hypothesis described above, comparisons will be made between user and manager perceptions. It is proposed wireless network managers and users will perceive security concerns differently. Specifically if managers have provided a reasonable level of protection for users, the users will not necessarily need to be

concerned about the security of the wireless network. Qualitative analysis will be employed in an effort to investigate these relationships, see Figure 3.1c.

It is anticipated that even with the relatively small number of managers' responses, a clear direction will emerge that indicates users and managers have differing opinions regarding the most important factors in the decision to use wireless networks. In particular, if managers absorb the brunt of security threats then users will be less concerned about potential threats not because they don't view them as significant but rather simply because they are protected. Figure 3.2 depicts a flow diagram that represents how the survey data and the case study data will dovetail to provide for an increased understanding of wireless network security.

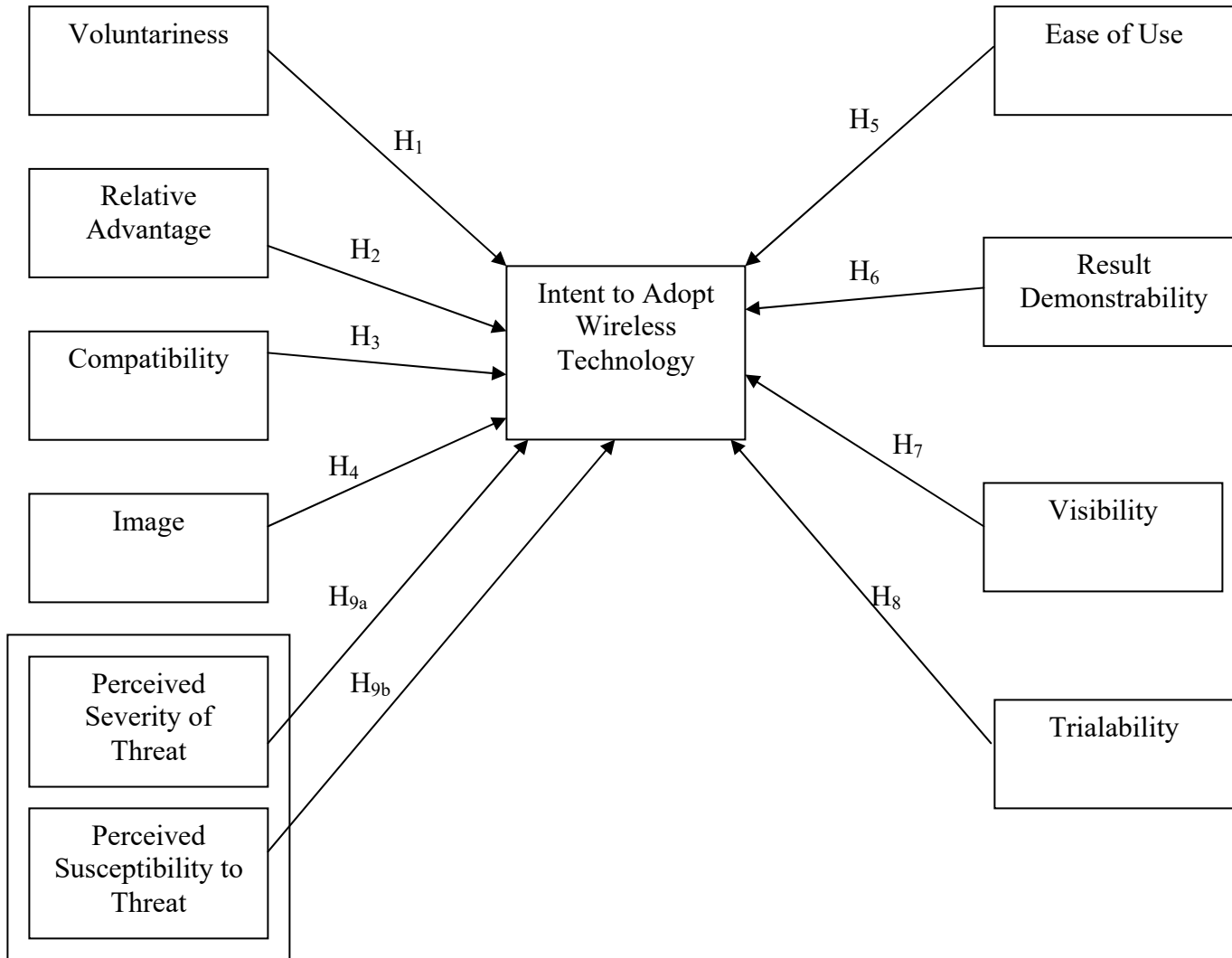


Figure 3.1: Proposed Model of “Propensity to Adopt” in Light of Security (user).

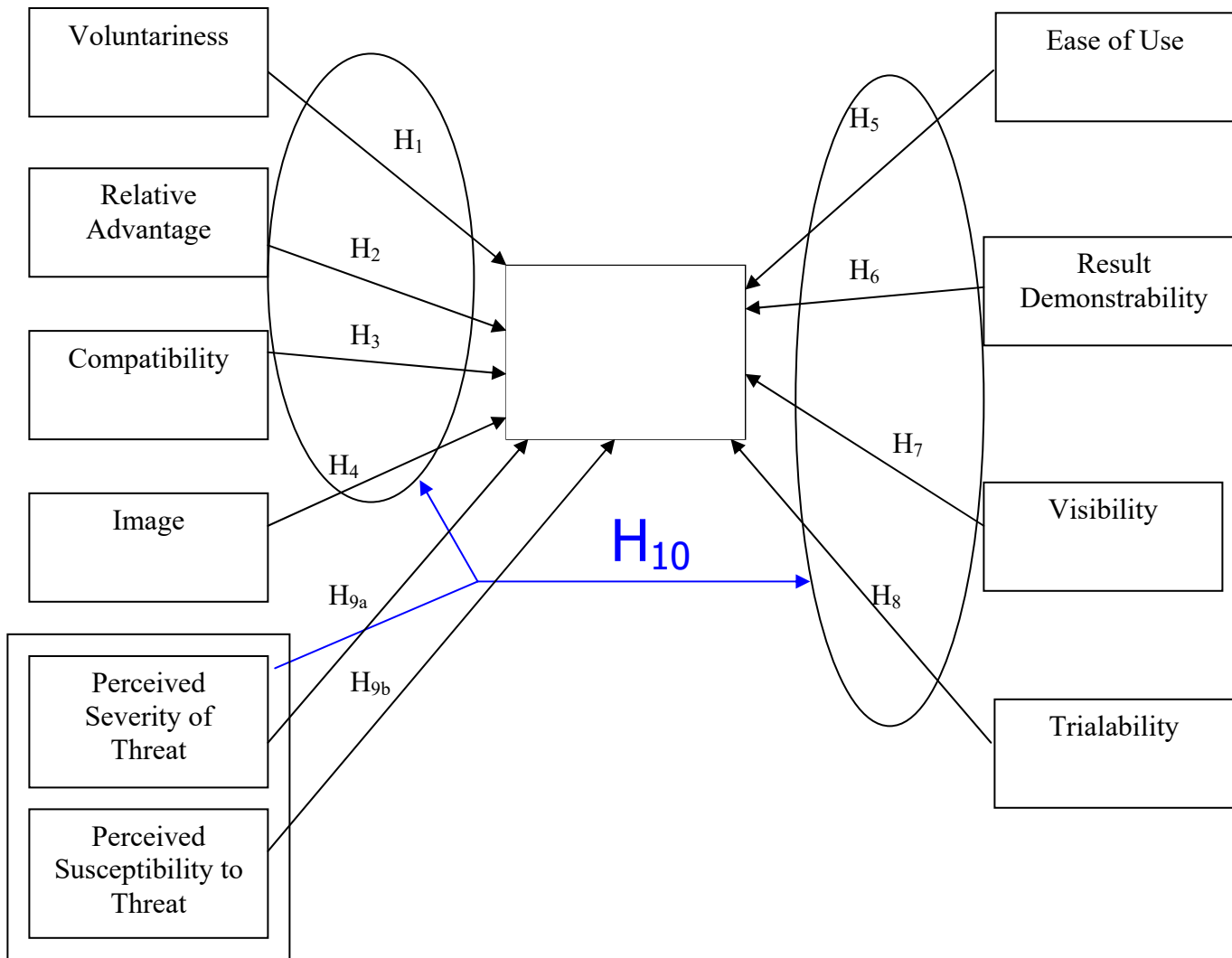


Figure 3.1a: Proposed Model of “Propensity to Adopt” in Light of Security (user).

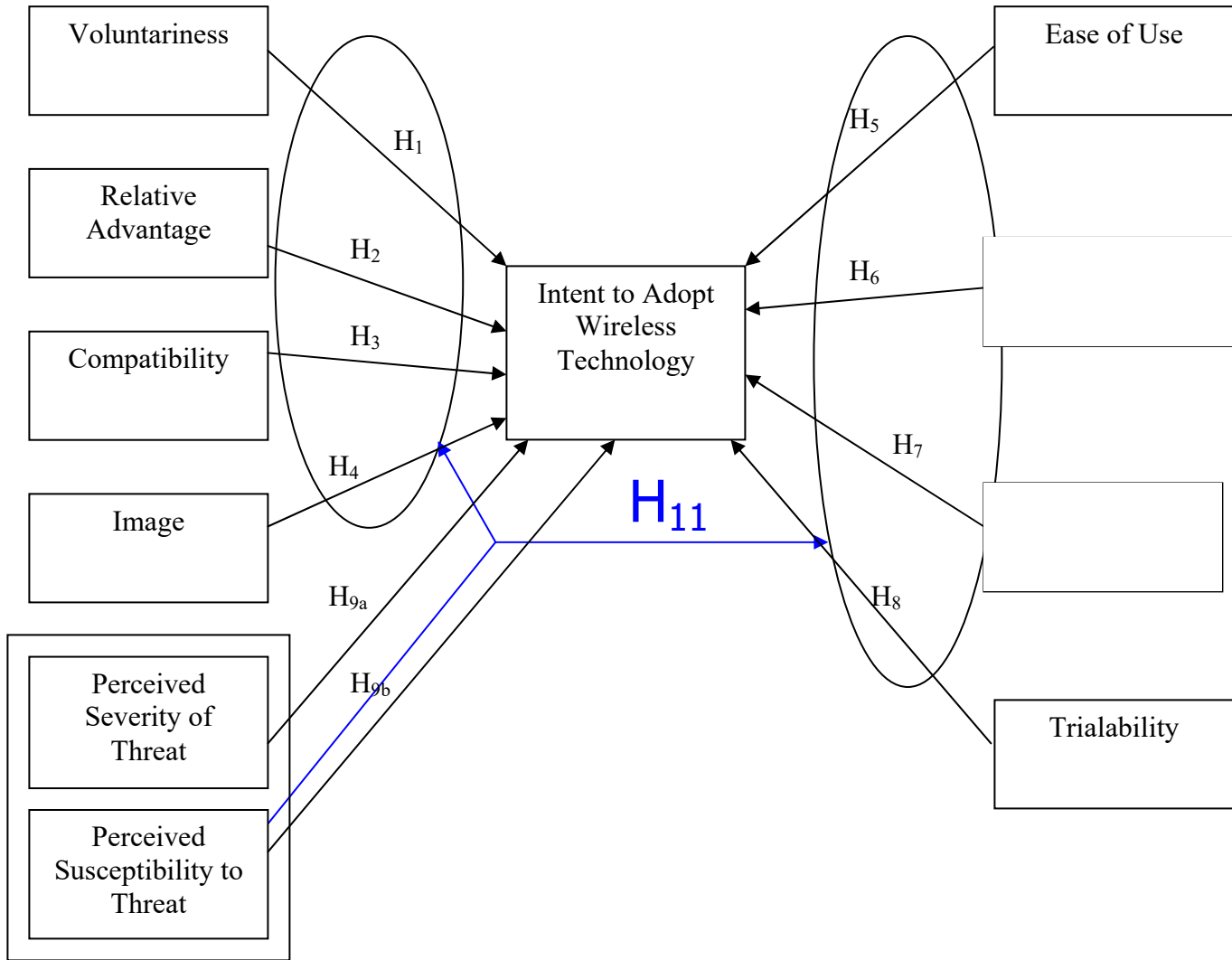


Figure 3.1b: Proposed Model of “Propensity to Adopt” in Light of Security (manager).

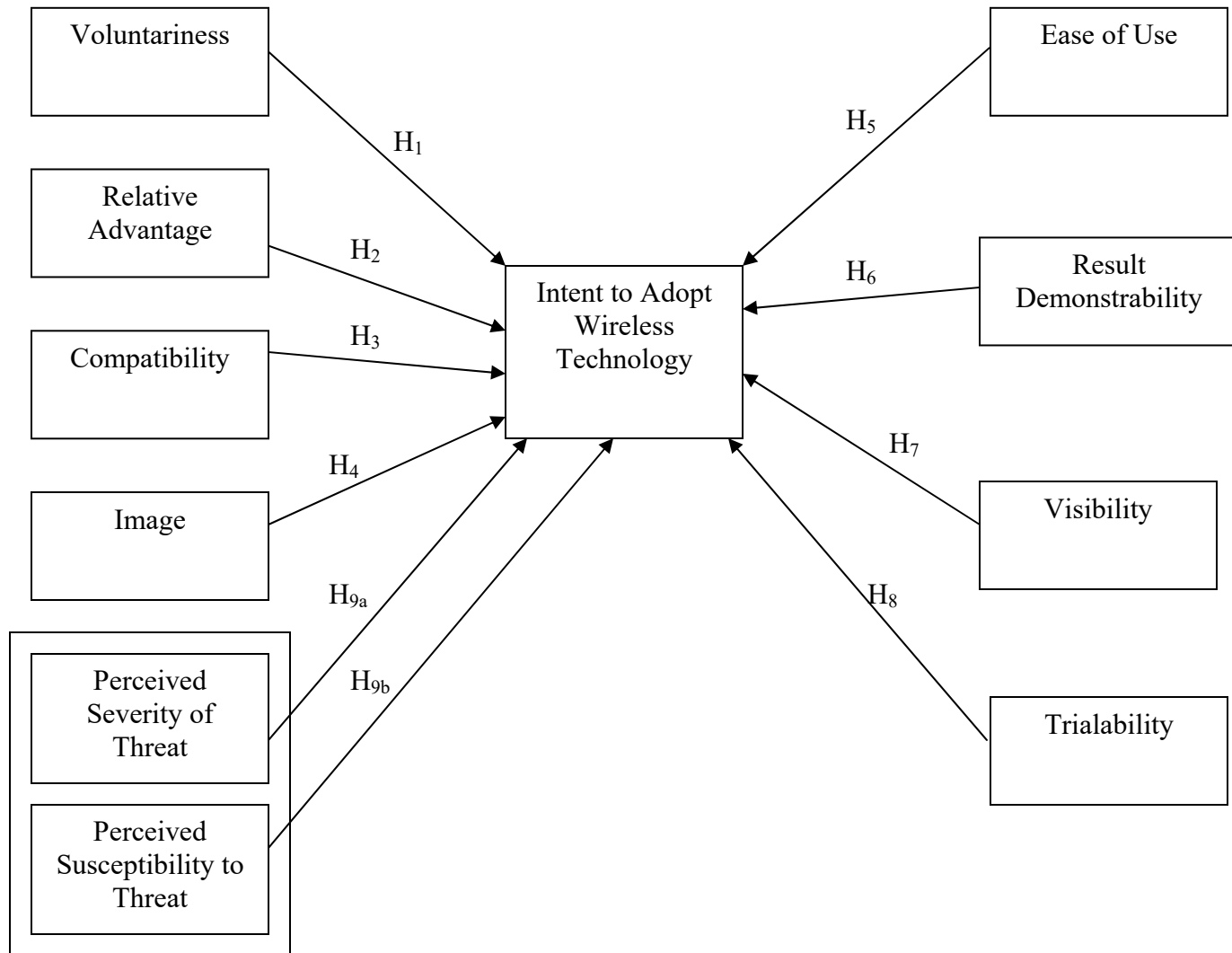


Figure 3.1c: Proposed Model of “Propensity to Adopt” in Light of Security (manager).



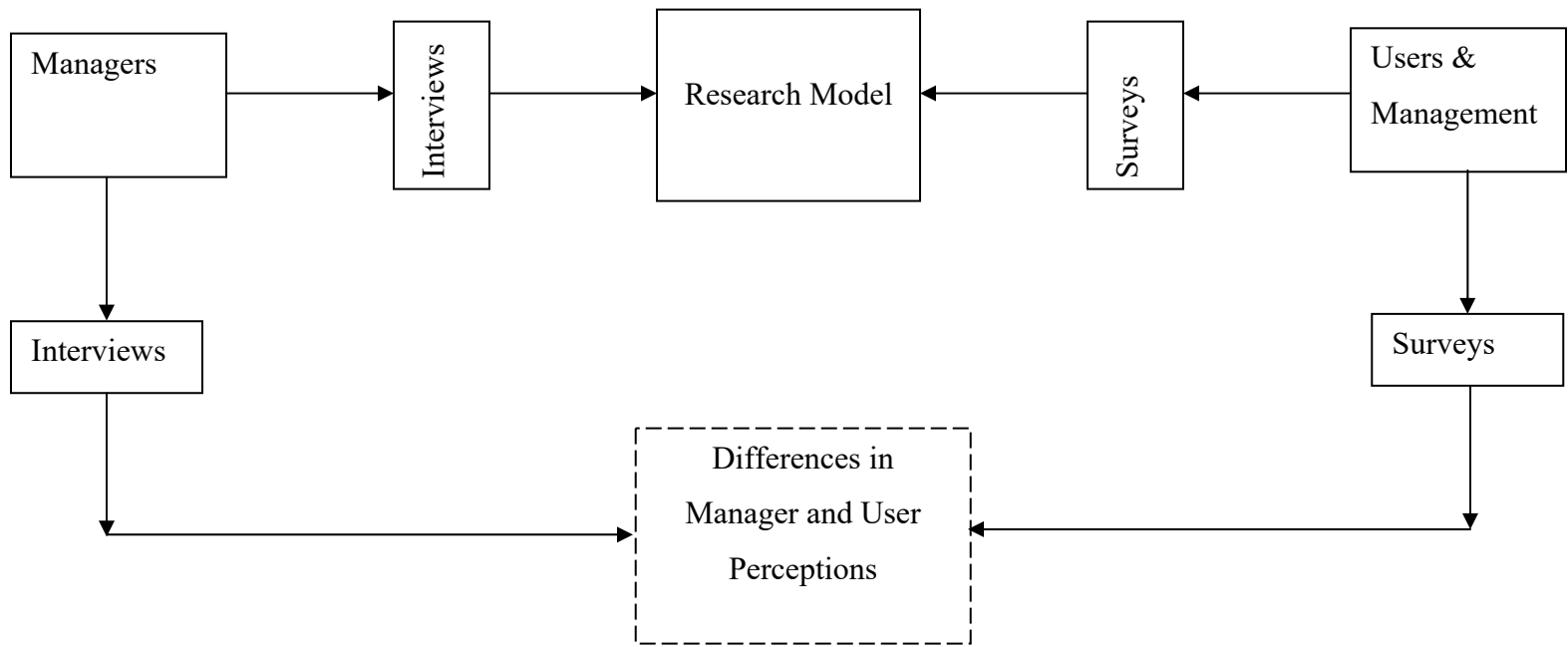


Figure 3.2: Flow Diagram of Research.

## Statistical Techniques

In order to determine if there is enough statistical evidence to reject the null hypotheses, logistic regression will be employed. Prior to the use of logistic regression, factor analysis will be utilized to ensure that the previously validated scales from the works of (Moore et al., 1991) and (Witte et al., 1996) are valid under the context and conditions in which they are being used.

### Factor Analysis

Exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) are two important types of factor analysis. EFA is conducive to research in which there is a dearth of recognized patterns identified in the data (Gerbing & Anderson, 1988). However, in areas where more established relationships and models are in existence, CFA is the appropriate technique (Hair Jr. et al., 1998; Sharma, 1996). Moore & Benbasat (1991), developed their items “to be as general as possible” and further suggest that “rewording by substituting the names of different IT innovations” could be done with the caution that additional confirmation of the constructs “would be prudent” (p. 211). Accordingly, CFA will be employed to ensure the validity of these previously validated instruments in a new situation.

### Logistic Regression

Both discriminant analysis and logistic regression are sound statistical approaches which can be used to differentiate between groups when a dependent variable is dichotomous or multi-chotomous. Both techniques essentially provide a mechanism to

determine if one or more variables provide a statistically significant manner in which to predict group membership. Both methods involve “multivariate analysis and nonlinear optimization” and, as such, both techniques are “inherently difficult concepts” (Albright, Winston, & Zappe, 2002, p. 834).

While discriminant analysis is based on “statistical distance, an intuitive concept that can be shown graphically” (Albright et al., 2002, p. 834); logistic regression, based on the logit function, is somewhat less intuitive. However, the key advantage in employing logistic regression techniques is that the mathematical model provides estimates of the probabilities of group membership as opposed to simply group membership as is the case in discriminant analysis; in addition, “its output is more in line with the familiar multiple regression output” (Albright et al., 2002, p. 834). In addition, logistic regression is more appropriate in many situations as it “does not face these strict assumptions [multivariate normality and equal variance-covariance matrices across groups] and is more robust when these assumptions are not met, making its application appropriate in many more situations” (Hair Jr. et al., 1998, p. 276). The logistic regression model is becoming more important to many statisticians and researchers and, consequently, there is a great deal of research being conducted using the model (Aczel, 1999). Because of the aforementioned advantages and the fact that diffusion at the individual level of analysis can be measured as a multi-chotomous variable, logistic regression will play an instrumental role in the statistical analysis of the data collected via survey.

In order to assess the statistical significance of the model, the chi-squared test and the Hosmer and Lemeshow statistic for goodness of fit can be employed; while the pseudo  $R^2$  can be used to assess the overall model fit (Hair Jr. et al., 1998).

Several statistics will be used in determining the overall effectiveness and fit of the final model. The Cox & Snell or the Nagelkerke  $R^2$  will be used to calculate an approximate  $R^2$ . The Wald Statistic will be used to test the significance of a single predictor. The odds ratio will be used to assess the effects of a dichotomous independent variable on the dependent variable in comparison to the reference group for the independent variable. The -2 Log Likelihood as well as the Hosmer-Lemeshow statistic for goodness of fit can be used to assess the overall fit of the model.

### **Sample Size Considerations**

Consistent with other researchers' efforts (cf. Plouffe et al., 2001), factor analysis will be employed in an effort to confirm the previously validated scales in the context of wireless networks. In a typical factor analysis, the minimum number of observations per variable is five while a ratio of ten-to-one is more acceptable (Hair Jr. et al., 1998). Further, it is recommended that researchers "should always try to obtain the highest cases-per-variable ratio to minimize the chances of over fitting the data (i.e., deriving factors that are sample specific with little generalizability)" (Hair Jr. et al., 1998). In this study the "short" scale as proposed by Moore and Benbasat (1991) will be used. This reduces the items in the scale from 39 to 25, which in turn will allow for a smaller sample size. However, there have been studies conducted using 52 of Moore and Benbasat's

items with as few as 15 respondents (Miller et al., 1997). Moore and Benbasat's reduced scale of 25 items will be combined with the six items from Witte et al. which then brings the total number of items to 31. If the goal of 400 respondents is achieved, a ratio of 12.9:1 will result. This will allow for a cushion in the number of useable responses; as the minimum number recommended by (Hair Jr. et al., 1998) is at least five respondents per variable while a ratio of ten-to-one is preferred.

### **Pilot Case Study**

This dissertation will employ the case study method in an effort to identify the factors that are considered in regard to wireless network security, develop an in-depth understanding of how decision makers utilize these factors, as well as provide an opportunity for comparing the perceptions of managers and users in regard to the perceived characteristics of innovating and security threats. Because case study research in MIS provides an "examination of a real-world MIS as it actually exists in its natural, real-world setting" (Lee, 1989, p. 34), it can be useful for the scientific community and practitioners alike. The scientific community gains an understanding of how IT artifacts are deployed and utilized in the practitioner community. The practitioner community benefits because it has the opportunity to be exposed to both exemplar situations that can provide insight on how to effectively do things and also failures that can be used as learning opportunities and provide insight on how to improve.

A pilot case study will be conducted on the campus of Mississippi State University (MSU) during spring semester 2005. Michael Argo, Compliance Officer, has

agreed to participate in the pilot study. Joe Whetstone, Vice President of Computing and Information Technology Services at Winona State University (WSU) and Stein Kristiansen, Network Technician at WSU were contacted in January 2005. Both Mr. Whetstone and Mr. Kristiansen indicated that they were willing to participate in the study. Phil Thorson, Director of IT Services, at Saint Cloud State University (SCSU) and Tony Sorteberg, Network Manager, at SCSU were contacted in December 2004. Both Mr. Thorson and Mr. Sorteberg agreed to participate in the study.

Several studies have employed a procedure whereby experts in a particular field are presented questions and then asked to provide feedback on the questions in an effort for the researchers to develop a better instrument (see Moore et al., 1991; Segars & Grover, 1998; Storey, Straub, Stewart, & Welke, 2000). Experts who were asked to refine and improve the instrument included three Business Information Systems professors as well as three network professionals. The case study questionnaire can be found in appendix B on page 215 of this document. Using a similar approach to (Moore et al., 1991; Segars et al., 1998; Storey et al., 2000), the pilot study will be used to refine the questions to be used in the structured interviews at other institutions. The Vice President of Computing and Information Technologies Services at one institution indicated his willingness to participate, as did the Director of Information Technology Services at another university.

Using the taxonomy of threats, network administrators will be interviewed to find the level of vulnerability posed by each of the threats. See appendix B on page 215 for specific details. Further, network administrators will be asked their opinions regarding

preparedness of their organizations as well as the level of preparedness of organizations similar to their own. Research has found that while people self reported that they themselves did not participate in software piracy, they reported that their colleagues did (Taylor & Shim, 1993). More recently, Schmidt & Arnett (2005) found that students perceived their contemporaries were less informed about and less prepared to deal with spyware. Other research finds that users often have a optimistic cognitive bias when comparing their level of vulnerability to security threats to others' vulnerability to the same threats (Rhee, Ryu, & Kim, 2005). Similar to the aforementioned findings, it is possible that managers will view themselves as more prepared than they view their competitors. This will be examined in the case study portion of this dissertation.

## CHAPTER IV

### DATA ANALYSIS

Chapter four presents a summary of the data analysis in effort to develop a deeper understanding of wireless network diffusion and security. The first major section of this chapter presents an analysis of the case study. The next portion of the chapter presents analysis of the survey research while the last portion synthesizes both the case and the survey research.

#### **Overview**

This dissertation has two main goals. The first involves extending Moore and Benbasat's (1991) PCI model. This goal was achieved by adding perceived severity of threat and perceived susceptibility to threat constructs (Witte et al., 1996) to the PCI model. The second goal is to extend the rich knowledge base regarding security considerations of wireless network implementations in a university environment. This goal was accomplished by utilizing the case study method. Additionally, the survey and case study results were synthesized in an effort to achieve a relative comparison of both end users' and IT professionals' perceptions of wireless security.



Two previously validated instruments were synthesized and revised to create a new instrument for extending the work of Moore and Benbasat. Logistic regression as well as multiple regression were used to provide statistical evidence in order to determine if Improvement Potential, Usage, Susceptibility and Severity of Threat, Image, Voluntariness, Visibility, and Trialability have an effect on innovation diffusion at the individual level of analysis. The analysis tests for interaction effects between the Susceptibility and Severity of Threat construct and the constructs of Improvement Potential, Usage, Susceptibility and Severity of Threat, Image, Voluntariness, Visibility, and Trialability.

As discussed in chapter three, this dissertation employs the case study method in an effort to identify the factors that are considered in regard to wireless network security. Additionally, the case study method was used to provide an opportunity for comparing the perceptions of managers and users in regard to the perceived characteristics of innovating and security threats. After a pilot case study, two additional case studies were conducted in an effort to gain deep knowledge of security issues relating to wireless network implementation.

This newly compiled knowledge will benefit the scientific and practitioner communities alike. It will assist the scientific community because it develops an increased understanding of how models developed in academia are deployed and utilized in the practitioner community. It will also further understanding in the practitioner community as it typifies successful wireless implementation. As part of developing this

in-depth understanding, several general research questions were considered and the following general research topics emerged:

1. Managers' level of concern,
2. Managers' implementation of technology,
3. Security factors,
4. Factors leading to wireless adoption at the organizational level, and
5. Managers' perceptions of security.

These general research topics were addressed in the interviews with IT professionals and are enumerated in subsequent sections. The specific interview questions can be found in appendix B starting on page 215.

### **Pilot Case Study Results**

The initial pilot case study interview was conducted on the campus of Mississippi State University (MSU) on June 16, 2005. Information Technology Services (ITS) Security and Compliance Officer, Mr. Michael Argo, was interviewed in his office. The main reasons for the pilot case study were to establish that the questions were sufficient to gain the deep knowledge needed for this part of the study and to become more effective and efficient when conducting the interviews. Although the questions were based on those used in previously published research (see Schmidt et al., 2004) and reviewed by several experts including three Business Information Systems professors, a need existed to use the questions with an actual security manager in a university environment.

The pilot study interview lasted two hours. Cognizant of the fact that many higher level information systems professionals might be very busy and not able to share

that amount of time with the interviewer, it was important to get Mr. Argo's thoughts on the best manner in which to reduce the overall time to complete the interview. Mr. Argo suggested that less time could be spent on the set of questions pertaining to the taxonomy of risks (the taxonomy can be found on page 218). Additionally it was suggested that the categories of risk were not always mutually exclusive. For instance, viruses were categorized as external, nonhuman, and deliberate. It clearly could be argued that viruses are internal, if released by an employee, human, if the employee wrote the code, and deliberate, if the intention was to cause harm to the company.

As a result of these factors, IT professionals who participated in the case study were not asked to specifically address each of the items on the list of threats. Rather they were asked to address the category they felt posed most potential threats to the security of their wireless network. Moreover, they were not "forced" to indicate a specific category when asked which of the threats was most harmful. Instead they were encouraged to use the taxonomy as a reference to discuss the subject of risk to their wireless network.

### **Case Study Results**

Mindful of the pilot case study, the actual case study was conducted involving IT professionals from two institutions. A purposeful sample that included campuses with highly unwired networks and Internet access was sought. A recent survey conducted by Intel found St. Cloud State University (SCSU) to be 50<sup>th</sup> in the list of top wireless universities in the United States (NotebookReview.com, 2005). Given that SCSU was selected as a top "unwired" university, their network management personnel were

selected as interview candidates. The aforementioned survey also included Winona State University (WSU) in its list of the top 50 wireless schools. WSU is a different type of unwired institution as all entering students are required to have a wireless enabled laptop or tablet PC with wireless capabilities. For these reasons, WSU was selected as the second case study location. Table 4.1 presents an overview of the data sources for the case study.

Table 4.1

## Data Sources for the Case Study

Case findings	
Interviews with IT Professionals	Questionnaires from IT Professionals
MSU = 1	MSU = 16
SCSU = 2	SCSU = 11
WSU = 4	WSU = 3
7 interviews	30 surveys

Initial contacts were made with SCSU and WSU in February 2005. The vice president of technology at each institution agreed to participate in the study. Mr. Joe Whetstone, Vice President of Computing and Information Technology Services at WSU, was interviewed on the phone from 8:50 am to 9:50 am on Wednesday, February 9, 2005. However, Mr. Whetstone was no longer an employee of WSU on September 8, 2005, when on-site interviews were being scheduled. Fortunately, Mr. David Gresham, the

current Vice President of Computing and Information Technology Services at WSU, was willing to be interviewed. As a result of the initial phone interview with Mr. Whetstone and his subsequent departure, this dissertation will have some areas that are addressed by two separate vice presidents from WSU. Table 4.2 provides a brief overview of the interviews.

Table 4.2

## Case Study Interview Details

<b>Name</b>	<b>Title &amp; level</b>	<b>University</b>	<b>Interview Date</b>	<b>Interview Length</b>	<b>Comments</b>
Michael Argo	ITS Security & Compliance Officer – 1 level below the “Head of ITS”	MSU	6-16-05	2 hours	Pilot interview.
Phil Thorson	Director Information Technology Services – 1 level below the “Dean, Learning Resources & Technology Services”	SCSU	8-29-05	1 ½ hours with 2 additional 10 minute meetings and 1 email	
Darrin Printy	IT Security Coordinator – 2 levels below the “Dean, Learning Resources & Technology Services”	SCSU	9-13-05	1 hour and 15 minutes	
Joe Whetstone	Vice President of Computing and Information Technology	WSU	2-9-05	1 hour	A phone interview was conducted on 2-9-05, 8:50 am – 9:50 am.

<b>Name</b>	<b>Title &amp; level</b>	<b>University</b>	<b>Interview Date</b>	<b>Interview Length</b>	<b>Comments</b>
					No longer an employee of WSU on September 8, 2005 when interviews were being scheduled.
David Gresham	Vice President of Computing and Information Technology	WSU	9-21-05 (brief face to face) 10-7-05 (phone)	10 minutes face to face and 35 minutes on the phone	The new Vice President of Computing and Information Technology.
Stein Kristiansen	Network Technician in charge of wireless – 2 levels below the “Vice President of Computing and Information Technology”	WSU	2-3-05 (phone) 9-21-05 (face to face)	1 hour and 45 minutes	
Dean Feller	Manager, Technical Support Center – 1 level below the “Vice President of Computing and Information Technology”	WSU	9-22-05	45 minutes	

### Managers’ Level of Concern

Managers are concerned for the overall security of their networks. However, as D. Printy put it, “there is a bigger concern that someone breaks in and steals a laptop than

there is of someone breaking into the system” (personal communication, September 13, 2005). P. Thorson went so far as to say that he trusts some wireless networks more than some wired networks because many wired networks are not encrypted and not tested as much; however, he was also quick to point out that he is VERY careful when using wireless networks in public areas such as hotels (personal communication, August 29, 2005).

Although authentication and encryption provide some level of security, wireless networks are inherently less secure than wired networks. D. Gresham wouldn't advise the use of wireless for online banking, but admitted that he uses wireless for that purpose; as he put it, “I wouldn't advise it – but I do it” (personal communication, October 7, 2005). Even the self proclaimed “super paranoid” M. Argo notes that with the VPN in place using the wireless network for banking could be as safe as going through a teller line in a bank (personal communication, June 16, 2005). In a similar line of reasoning, S. Kristiansen commented that with any online transaction personal information might be compromised with such activities as *man in the middle attacks* (personal communication, September 21, 2005). Table 4.3 details the responses given during the interviews.

Table 4.3

## Interviewee Responses

Question	Do you consider the wireless network secure?
Michael Argo	<ul style="list-style-type: none"> <li>• Yes</li> <li>• Only two MACs per port are allowed</li> <li>• This allows only two machines to get wireless access if a rouge access point were to be deployed</li> </ul>
Phil Thorson	<ul style="list-style-type: none"> <li>• Yes – but there are smart students out there (who might try to hack)</li> <li>• The MN legislature would rate it a 9 of 10</li> <li>• I would rate it an 8 of 10</li> </ul>
Darrin Printy	<ul style="list-style-type: none"> <li>• Yes – we didn't deploy it until we had security solutions in place</li> <li>• We didn't jump in 5-6 years ago – we waited for better solutions</li> <li>•</li> </ul>
Joe Whetstone	<ul style="list-style-type: none"> <li>• An initial phone interview was conducted on 2-9-05, 8:50 am – 9:50 am. However, he was no longer an employee of WSU on September 8, 2005 when interviews were being scheduled. As a result, Mr. Whetstone did not provide an answer to this question.</li> </ul>
David Gresham	<ul style="list-style-type: none"> <li>• Yes, but there are no mission critical applications that depend on wireless</li> </ul>
Stein Kristiansen	<ul style="list-style-type: none"> <li>• Not fair to ask</li> <li>• Relatively secure</li> <li>• Wouldn't want to say anything is secure – there are degrees of security</li> <li>• Nothing is 100% secure unless it is turned off and even then it might not be totally secure</li> </ul>
Dean Feller	<ul style="list-style-type: none"> <li>• Our network is very secure</li> </ul>



### Managers' Implementation of Technology

According to P. Thorson, SCSU employees a variety of security mechanisms to proved a secure wireless environment. For instance, virtual private networks (VPN) are used and user privileges are mapped to one of six user types each of which allow various levels of privilege to users (personal communication, August 29, 2005). Mr. Thorson also commented on the Minnesota State Colleges and Universities (MnSCU) audit and indicated that the results put SCSU at a nine of ten for wireless security, while he would rate it at an eight. This is quite impressive as a ten would be considered the best possible security. M. Argo was very forthcoming regarding wireless security when he said, “the network is as secure as it can be with the technology we have – but there are no guarantees that it will not be compromised” (personal communication, June 16, 2005).

IT professionals were asked if anyone had ever broken into their wireless network, and the standard response was “no”. However, there were other potential security concerns. For example, at one point in time SCSU had as many as 30-50 rogue access points. Based on this unacceptable number of rogue access points, they now have a procedure in place that uses existing access points to locate a rogue and then send a page notification to a wireless network professional who is authorized to handle the problem (personal communication, August 29, 2005). Table 4.4 details the responses given during the interviews.

Table 4.4

## Interviewee Responses

Question	Has anyone ever broken into the wireless network?
Michael Argo	<ul style="list-style-type: none"> <li>• Perhaps on weekends</li> <li>• ERC &amp; others are hesitant to reveal if a break-in occurs</li> </ul>
Phil Thorson	<ul style="list-style-type: none"> <li>• No</li> <li>• 30-50 rogue points at any given time</li> <li>• Part of the audit was to find a rogue point               <ul style="list-style-type: none"> <li>○ Sends a page to a network manager</li> <li>○ Based on existing access points it can locate the rogue point and draw it on a campus map</li> </ul> </li> </ul>
Darrin Printy	<ul style="list-style-type: none"> <li>• No</li> </ul>
Joe Whetstone	<p>An initial phone interview was conducted on 2-9-05, 8:50 am – 9:50 am. However, he was no longer an employee of WSU on September 8, 2005 when interviews were being scheduled. As a result, Mr. Whetstone did not provide an answer to this question.</p>
David Gresham	<ul style="list-style-type: none"> <li>• Not that I know of</li> </ul>
Stein Kristiansen	<ul style="list-style-type: none"> <li>• No</li> </ul>
Dean Feller	<ul style="list-style-type: none"> <li>• No</li> <li>• We only allow our laptops on the network</li> </ul>

WSU is fortunate in the sense that they only have four hardware configurations that must be supported at any given time. Their laptops supplied to incoming freshman

and transfer students are on a two year cycle with a choice of a MAC or tablet PC. According to D. Gresham, because of this relatively low number of configurations, WSU is better able to utilize their technology resources by redirecting the staff that would otherwise need to address access for a large number of configurations (personal communication, October 7, 2005). When asked if his wireless network was secure, S. Kristiansen replied by saying, “that is not a fair question to ask” and he continued to say, “I wouldn’t want to say anything is secure – there are just degrees of security” and “nothing is 100% secure – unless it is turned off and even then it might be questionable” (personal communication, September 21, 2005).

#### Security Factors

Many security experts warn that the risk posed by insiders is greater than the risk posed by outsiders. Network professionals were shown a taxonomy of threats and asked to discuss which of the threats posed the most potential security concern. Table 4.5 presents an abbreviated taxonomy of risks.

Table 4.5

## Abbreviated Taxonomy of Threats

<b>Location</b>	<b>Source</b>	<b>Intent</b>
I. Internal		
	a. Human	
		i. Deliberate
		ii. Unintentional
	b. Nonhuman	
		i. Deliberate
		ii. Unintentional
II. External		
	a. Human	
		i. Deliberate
		ii. Unintentional
	b. Nonhuman	
		i. Deliberate
		ii. Unintentional

One of the difficulties of using a taxonomy of risks relates to the fact that several of the risks might actually be interpreted to be in more than one category. This lack of mutual exclusivity led some interviewees to have difficulty in stating which of the categories of risk posed the largest problems to network managers. For example, S. Kristiansen commented that self replicating worms, such as MS Blaster, originated as an external, human, and deliberate risk but then progressed to an internal, human, and unintentional risk as people without the proper security patches allowed the worm to spread throughout the network (personal communication, September 21, 2005).

Another potential difficulty with utilizing this, or any, taxonomy of risks involves the fact that, due to the increasing number of threats in the computing environment, it is difficult to develop collectively exhaustive categories. One potential solution is to

include an “other” category. However, it is likely that the other category would be the most populous. For example, D. Printy expressed concern about never achieving a 100% protection level because there are new threats that emerge every week (personal communication, September 13, 2005). As expected, it was not possible for interviewees to easily characterize their exposure to the threats listed in the taxonomy. In fact, it was determined during the pilot case study that it would be difficult to expect an interviewee to accurately and concisely characterize threats using a taxonomy. Therefore, during the interview process the taxonomy was used as a starting point for a discussion on threats, as opposed to its initial purpose, which was to simply identify the most significant threats according to each interviewee.

Due in part to the fact that it was not possible to develop a taxonomy that was meaningful while at the same time encompassing a mutually exclusive and collectively exhaustive list of threats, a specific category did not emerge as presenting the most problems. However, there did seem to be particular concern in regard to internal – human threats. As D. Gresham put it, “we have 800 faculty and staff and 7,500 students all with some inside knowledge of our systems and each is a potential hacker that might cause either malicious or accidental damage” (personal communication, October 7, 2005).

S. Kristiansen expressed a great level of concern for carelessness of people on the network that can further the propagation of self replicating worms and other malware such as MS Blaster (personal communication, September 21, 2005). He then lamented that one of the reasons that we as a society are so vulnerable to such infestations is due to

the fact that so many people use Microsoft products. He likened it to a stand of timber that contains 90% Red Pines where Red Pine blight goes through and destroys 90% of the stand. The lack of biodiversity in a stand of timber can create a larger degree of susceptibility to risks in the environment; in a similar way, the world is more susceptible to malware targeted at Microsoft products because of Microsoft's dominance in the industry.

Table 4.6 lists some common security mechanisms that respondents identified which are employed to secure the wireless networks. VPN and firewalls are common tools. LEAP is a Cisco proprietary authentication mechanism that, according to S. Kristiansen, won't work without WSU's laptop program, because the laptop program only allows for approximately four different configurations to be supported at any given time (personal communication, September 21, 2005). Unfortunately, in the ever changing computer security landscape there are efforts underway to crack LEAP.

Table 4.6

## Security Mechanisms Employed

University	Mechanisms Employed
SCSU	VPN, Privilege Levels, Firewall
WSU	LEAP, VPN, Firewall

### Factors of Adoption at the Organizational Level

Viewed from a holistic perspective, the ultimate usage of wireless networks in the university setting is a “contingent innovation-decision” because an individual can only make the accept or reject decision after a prior innovation decision (Rogers, 1995).

Figure 4.1 shows the relationship of the contingent innovation decision where both network managers and users have an effect on the ultimate adoption decision.

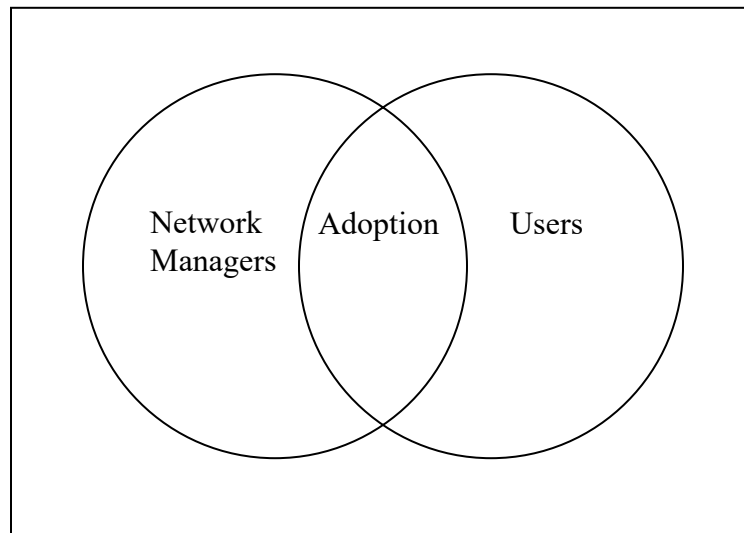


Figure 4.1: The Contingent Innovation Decision

In many contingent innovation decisions, individual users have at least some level of autonomy in their level of use of the innovation. This autonomy stems from their individual level of use. For instance, some users will exhibit a high level of use and even use the innovation in a manner that expands its capabilities, while others will limit their use to the most basic functions (Carlson et al., 1999).

From the network managers' and decision makers' perspective, stakeholder demand was instrumental in the contingent innovation decision to use wireless. P. Thorson remarked that his niece and nephew are college students and have a keen sense of awareness of technology issues and want the latest technological features available to them (personal communication, August 29, 2005). While cost savings might be a reason for some organizations to use wireless instead of a wired infrastructure, it wasn't at WSU because when they build a new building or renovate an existing building they include both wired and wireless infrastructure. Wireless is also complementary to the wired network at SCSU. The original renovation plans for Centennial Hall, which will become the new home to the College of Business, included two data ports per office, but now, with wireless access, there will only be one wired port per office (personal communication, August 29, 2005). So, in this case, wireless may actually save money in the renovation process.

From the users' perspective, convenience and ease of use seems to emerge as clear reasons why users adopt wireless in the second half of the contingent innovation decision. S. Kristiansen feels that users moved remarkably fast from a point of being impressed by the "whiz bang" factor of wireless to feeling upset if they experience dead spots on campus. He even went so far as to say that wireless was the fastest technology adoption by end users that he has ever seen, and once it was in place it was like it had always been there (personal communication, September 21, 2005). D. Gresham mentioned that the wireless network is like water or electricity in that it is assumed to be



running 24 hours a day seven days a week, and, if it isn't, users will become very upset (personal communication, October 7, 2005).

### Managers' Perceptions of Security

MnSCU recent security audit of member institutions included both SCSU and WSU. Representatives from both schools made mention of the audit but were reluctant to release any details regarding specific findings. All of the interviewees went through the same audit; this fact likely helped them to answer questions regarding their level of preparedness.

Viewed as a whole, which includes both two and four-year schools in the MnSCU system, the findings indicated that there was a general lack of preparedness. The MnSCU security audit refers to wireless technologies as new and fast changing but also states that wireless access creates a situation where there is increased risk for unauthorized access to computer systems and data. In fact, the official recommendation made to Dr. James McCormick, Chancellor of MnSCU, was to "disable all wireless networks that lack strong authentication and encryption controls" (Minnesota Office of the Legislative Auditor, 2005, p. 3). However, it should be noted that there are large differences between the findings for two and four-year institutions. For instance, D. Gresham rated all the four-year schools in the MnSCU system between seven and nine (out of ten) in terms of preparedness to deal with security threats to their wireless networks whereas the two-year schools were rated at a five or less (personal communication, October 7, 2005). When asked to elaborate on the details of the discrepancy, he stated that several of the two-year

schools simply have a small number of employees who are charged to handle all IT related issues even though there are not actual IT departments (personal communication, October 7, 2005).

Taylor & Shim (1993) found that while people self reported that they themselves did not participate in software piracy, they suspected that their colleagues did participate in software piracy. Recently, Schmidt & Arnett (2005) found that students perceived their contemporaries were less informed about and less prepared to deal with spyware. Interestingly, both of these studies found that respondents view themselves as “better” than their associates (i.e. I don’t pirate software but my colleagues do and I know more about computer security than do my associates). In a similar line of reasoning it would be interesting to ask interviewees if they view themselves as more prepared than they view their competitors. To that end, the following two questions were asked:

Considering the preceding list of threats as well as your own list of threats, how well is your organization prepared to deal with these threats?

Not prepared								Very prepared	
1	2	3	4	5	6	7	8	9	10

Please elaborate:

and

Considering the preceding list of threats as well as your own list of threats, how well are other organizations similar to yours prepared to deal with these threats?

Not prepared								Very prepared	
1	2	3	4	5	6	7	8	9	10

Please elaborate:

It was not surprising to find that every IT professional perceived his wireless network to be more secure than wireless networks in similar organizations, or at least higher than some in the case of David Gresham. The MnSCU report did not release specific details on the level of preparedness. It did however indicate that there are various strong areas as well as much room for improvement. There seemed to be a consensus that the two-year schools are much less prepared than the four-year schools. In fact, three of the five interviewees specifically mentioned their opinion that the two-year schools were lacking in the IT area. For example, D. Gresham indicated that several of the smaller two-year schools didn't even have an IT department (personal communication, October 7, 2005). Table 4.7 summarizes managers' perceived level of preparedness.

Table 4.7

## Perceived Preparedness

<b>Name</b>	<b>University</b>	<b>Your level</b>	<b>Others' level</b>
Michael Argo	MSU	9	8
Phil Thorson	SCSU	8	5
Darrin Printy	SCSU	9	4.5
David Gresham	WSU	8	7, 8, 9 But much lower for two-year MnSCU schools
Stein Kristiansen	WSU	6	3
Dean Feller	WSU	7	4
Mean rating		7.8	5.4

According to D. Gresham, many such schools purchased several wireless access points from local retail outlets and plugged them in without further security considerations (personal communication, October 7, 2005). D. Printy in referencing MnSCU institutions remarked that, "some places are in pretty rough shape" and further lamented that there are many two-year schools that purchased and installed wireless access points without regard to security (personal communication, September 13, 2005). S. Kristiansen indicated that two-year schools were definitely understaffed in their IT departments (personal communication, September 21, 2005), which may explain why they are thought to be less prepared to deal with threats to their wireless networks.

IT professionals were very confident regarding their level of security in regard to their wireless networks. Yet in one way or another, all seven IT professionals

interviewed made the admission that they don't have perfect security because, in the "one-upsmanship" world of computer security, what is perfectly secured today is unlikely to be perfectly secured tomorrow. M. Argo remarked, "the only way to be 100% secure is to unplug everything from the network" (personal communication, June 16, 2005). D. Printy remarked that providing security in general, and wireless security specifically, is a constant battle and what is considered a ten today will not be a ten tomorrow (personal communication, September 13, 2005).

S. Kristiansen voiced a bit more concern for the security of his and other organization's wireless networks. "Even though we have a myriad of things such as firewalls, LEAP, VPNs, and others, the problem is that we don't know what else is coming." Perhaps, as the network technician in charge of wireless, he has seen more security related incidents. Security is a reactive situation. Adequate protection is in place and then someone breaks it, then security professionals react, and hence goes the cycle. Further, every new case sets a new precedent, but the best solution might be more unclear than clear. S. Kristiansen made a point that things have changed for network professionals in the last few years by stating, "10-12 years ago we were just trying to get the lights to turn green. Now I have to wonder if an email sent to me by the Recording Industry Association of America (RIAA) will eventually show up in court" (personal communication, September 21, 2005).

Although the sample size of IT professionals (n=30) did not allow for a factor analysis, some evidence did emerge to indicate how security professionals thought about their intent to adopt wireless. Specifically IT professionals are concerned as to Perceived

Severity of Threat and Perceived Susceptibility to Threat when considering the decision to adopt wireless or not. However, a T-test for equality of means revealed that end users shared a similar level of concern with IT professionals. Table 4.8 depicts the T-test results. Figure 4.2 depicts a model (revised from figure 3.1c) that depicts the relationship between adoption and security threats.

Table 4.8

## Individual T-test results

		Independent Samples Test				
		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
SecuritySevere	Equal variances assumed	-.153	506	.878	-.044	.289
	Equal variances not assumed	-.161	30.624	.873	-.044	.275
SecuritySerious	Equal variances assumed	-.526	506	.599	-.156	.297
	Equal variances not assumed	-.542	30.466	.592	-.156	.288
SecuritySignificant	Equal variances assumed	-.732	507	.464	-.209	.285
	Equal variances not assumed	-.689	29.804	.496	-.209	.303
DataWrongHands	Equal variances assumed	.606	506	.545	.173	.285
	Equal variances not assumed	.541	29.492	.593	.173	.319
NegConLikely	Equal variances assumed	1.701	508	.089	.450	.264
	Equal variances not assumed	1.947	31.402	.061	.450	.231
NegConPoss	Equal variances assumed	1.383	508	.167	.390	.282
	Equal variances not assumed	1.269	29.645	.214	.390	.307

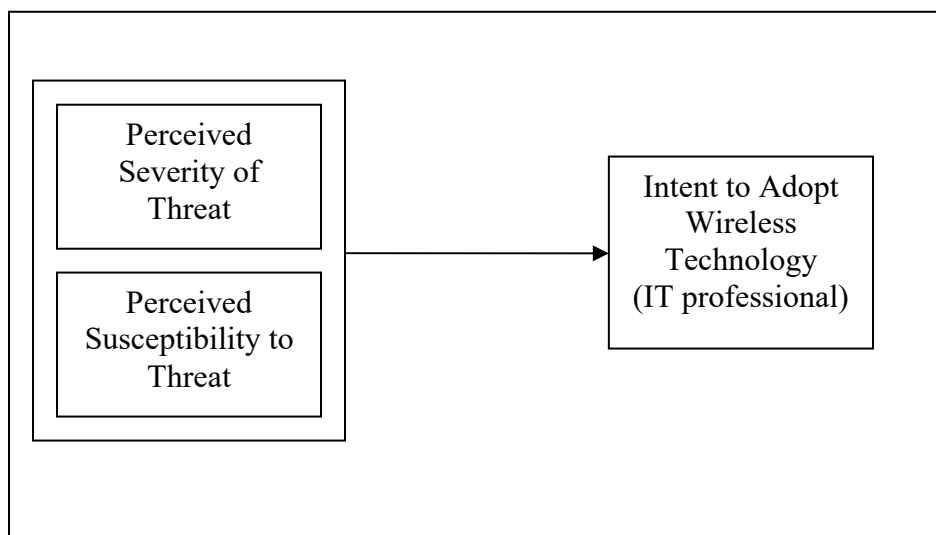


Figure 4.2: Revised Model for IT Professionals

Additional research is needed to address the significance of the constructs of an IT professional's perspective. Specifically, surveys from more IT professionals are required to conduct an analysis.

### Survey Results

A paper based questionnaire was given to students of two universities. In total 492 surveys were collected. The questionnaire can be viewed in appendix A starting on page 208. The initial goal was to get 200 usable responses from Mississippi State University and 200 usable responses from Winona State University. This goal of 200 responses from each university was achieved in September 2005. Table 4.9 summarizes the source of the 492 surveys collected.

Table 4.9

## Data Sources

<b>Location</b>	<b>Date</b>	<b>Number of surveys</b>
Mississippi State University (MSU)	9-26-05	275
Winona State University (WSU)	9-21-05 and 9-22-05	217
	<b>Total Surveys</b>	<b>492</b>

As with most survey research, there were issues with missing data that needed attention in this study. In addressing these issues the researchers' primary concern is to understand the factors that lead to the missing data (Hair Jr. et al., 1998). Among the major concerns are hidden biases that may occur because respondents are not comfortable answering certain questions and the practical implications on sample size. After a thorough analysis of the missing data it was found that five respondents failed to complete an entire page of the survey. This may have been due to the fact that the survey was copied front to back. In any case, a respondent who missed an entire page was likely not very careful when answering the questions. To negate the possible negative effects of such surveys, those five surveys (survey # 84, 104, 159, 368, and 395) were not used in the final analysis. Such a remedy is one of four possible courses of action when dealing with missing data (Hair Jr. et al., 1998).

Additionally, six respondents did not provide a response for the dependent variable. As a result, those six (survey # 144, 175, 176, 179, 192, and 206) were dropped



from final analysis. In total, 11 surveys were deleted from the data set. The final number of usable surveys was 481.

Twenty-two other respondents did not provide a response for one independent variable. Because these 22 respondents were missing only one of 31 (3.2%) independent variables, their records were retained. Specifically, of the 22 missing data points, there was one variable (SeeOthers) that was omitted by three respondents, there were six variables omitted by two respondents (Profile, FitsStyle, EasyToUse, DiffExplainBene, SecuritySevere, and SecuritySerious), and seven variables (Compatible, ProfRequire, Control, SecuritySignificant, ApparentResults, and DataWrongHands) that were omitted by one respondent each.

Imputation is one possible method to account for missing data (Hair Jr. et al., 1998). Considering the fact that there were 481 usable surveys, each with 31 independent variables, there were 14,911 ( $481 \times 31$ ) possible data points. Twenty-two missing data points corresponds to 0.15% ( $22/14,911$ ) of the possible missing values. Further, the 22 missing values were spread among 13 independent variables. Although this missing data is a cause for concern, imputation was used to deal with the missing data. The process of mean imputation was used to replace the missing values with the mean value for that variable. Table 4.10 presents a summary of the missing data.

Table 4.10

## Summary of Missing Data and Action Taken

Number of surveys	Missing item(s)	Action taken
5	Missing a full page of variables	Removed from analysis
6	Missing the dependent variable	Removed from analysis
1	Missing 2 independent variables	Imputation was used in SPSS to account of these variables
21	Missing 1 independent variable	Imputation was used in SPSS to account of these variables

## Sample Characteristics

Respondents were recruited from three and five classes at MSU and WSU respectively. Table 4.11 presents a summary of the characteristics of the sample. Table 4.12 shows the number of valid responses for each variable, the range, the minimum and maximum value, the mean, and the standard deviation for each independent and dependent variable.

Table 4.11

## Selected Demographics of Respondents

Demographic	Characteristic
Age	92% are 18-23
Gender	57% male
Major	85% are business or technology majors
Classification	73% are juniors or seniors
Years using computers	95% have used computers 6 or more years
Years using wireless	Average 3 years
Number of computer classes taken	Average 4 classes
Own desktop	55% own a desktop
Own laptop	78% own a laptop

Table 4.12  
Descriptive Statistics

Descriptive Statistics						
	N	Range	Minimum	Maximum	Mean	Std. Deviation
ProfRequire	480	6	1	7	5.11	1.851
NotCompuls	481	6	1	7	4.61	1.832
Wquickly	481	6	1	7	5.31	1.552
ImprovQual	481	6	1	7	4.51	1.571
Ejob	481	6	1	7	5.31	1.508
Effective	480	6	1	7	4.75	1.582
Control	479	6	1	7	4.72	1.538
Compatable	479	6	1	7	4.61	1.485
FitsWork	481	6	1	7	5.35	1.359
FitsStyle	479	6	1	7	5.36	1.334
Prestige	481	6	1	7	3.61	1.549
Profile	479	6	1	7	3.67	1.551
Status	481	6	1	7	3.30	1.600
Clear	481	6	1	7	5.04	1.379
EasyToGet	481	6	1	7	4.78	1.486
EasyToUse	478	6	1	7	5.46	1.278
EasyOperate	481	6	1	7	5.43	1.338
TellOthers	481	6	1	7	5.28	1.286
CommConsequ	481	6	1	7	4.90	1.415
ApparentResults	480	6	1	7	5.08	1.267
DiffExplainBene	479	6	1	7	3.51	1.631
SeeOthers	478	6	1	7	5.18	1.415
NotVisable	481	6	1	7	2.91	1.582
ProperlyTry	481	6	1	7	3.78	1.557
PermittedToUse	481	6	1	7	3.02	1.612
SecuritySevere	479	6	1	7	4.02	1.488
SecuritySerious	479	6	1	7	4.30	1.525
SecuritySignificant	480	6	1	7	4.46	1.457
DataWrongHands	479	6	1	7	4.46	1.454
NegConLikely	481	6	1	7	3.31	1.370
NegConPoss	481	6	1	7	4.07	1.443
CheckAcct	481	5	0	5	1.34	1.021
CheckAcctNLH	481	2	0	2	1.16	.587
CheckAcctYN	481	1	0	1	.89	.308
SecConcern	474	9	1	10	6.47	2.456
Valid N (listwise)	451					

## Factor Analysis

SPSS version 13.0 for Windows was employed to conduct a factor analysis. The following procedures, as outlined by Garson (2005), were used in the factor analysis. Bartlett's Test of Sphericity indicated highly significant results (8771.124 with  $p < .000$ ). The Kaiser-Meyer-Olkin Measure of Sampling Adequacy was .872. Based on Kaiser's work, a measurement of .80 or above can be thought of as "meritorious" (Hair Jr. et al., 1998).

Principal components was used as the extraction method. Factors having an eigenvalue over 1.0 were retained. Varimax rotation was used to rotate the matrix (Torkzadeh & Dhillon, 2002). Several other rotation methods were also using in an effort to eliminate the cross loadings; however, Varimax rotation produced the best results. Missing values were replaced with the mean of that particular variable during the analysis via SPSS. Initially a confirmatory factor analysis (CFA) was run. Given the existence of research that has established relationships and models for given phenomena, CFA is the appropriate technique (Hair Jr. et al., 1998; Sharma, 1996). However, when the model is forced to include ten factors, as are present in the original works of Moore & Benbasat (1991) and Witte, Cameron, McKeon, & Berkowitz (1996), there are many significant cross-loadings. In table 4.13, primary loadings are in bold and the significant cross loadings are noted with italics.

Typically loadings of .4 or higher are considered significant (Garson, 2005; Hair Jr. et al., 1998) therefore, loadings of .4 or higher were considered in this analysis. Higher loadings indicate a stronger relationship between the items. Loadings between .4

and .5 are considered “important” while loadings of .5 or greater are considered “practically significant” (Hair Jr. et al., 1998). In the following analysis there were five loadings between .4 and .5, and were considered in the identification of the factors.

The following descriptions are found in Moore & Benbasat (1991). Relative Advantage is the degree to which an innovation is perceived as being better than its precursor. Ease of Use, originally termed complexity by Rogers, is the degree to which an innovation is perceived as being difficult to use. Image is the degree to which use of an innovation is perceived to enhance one’s image or status in one’s social system. Visibility, originally termed observability by Rogers, is the degree to which one observes others in the organization using the innovation. Compatibility is the degree to which an innovation is perceived as being consistent with the existing values, needs, and past experiences of potential adopters. Results Demonstrability is the tangibility of the results of using the innovation, including their observability and communicability. Voluntariness of Use is the degree to which use of the innovation is perceived as being voluntary, or of free will. Trialability is the degree to which an innovation may be experimented with before adoption.

Perceived Severity of Threat and Perceived Susceptibility to Threat are two specific constructs relating to threats. Perceived Susceptibility can be thought of as beliefs about one’s risk of experiencing a threat while Perceived Severity is defined as beliefs about the importance or magnitude of the threat (Witte et al., 1996). Appendix D lists the questions that led to the items presented in table 4.13.

Table 4.13

## CFA Results

Rotated Component Matrix										
	Factor									
	voluntariness	relative advantage	compatibility	image	ease of use	result demonstrability	visibility	trialability	severity of threat	susceptibility to threat
<b>ProfRequire</b>	-.117	.003	-.006	-.046	.028	-.059	.026	<b>.880</b>	-.093	-.033
<b>NotCompuls</b>	-.319	-.032	.068	-.199	-.120	.074	-.075	<b>.752</b>	.024	-.070
<b>Wquickly</b>	<b>.728</b>	.255	.093	.045	.137	-.067	.066	-.036	.001	.154
<b>ImprovQual</b>	<b>.791</b>	.196	-.050	.226	.006	-.006	.017	-.246	.092	-.055
<b>Ejob</b>	<b>.762</b>	.226	-.025	.055	.233	.024	.096	-.046	.021	.183
<b>Effective</b>	<b>.854</b>	.174	.013	.180	.084	.003	.063	-.153	.045	.074
<b>Control</b>	<b>.765</b>	.163	-.012	.203	.215	.017	.004	-.084	.042	.055
<b>Compatible</b>	.365	.254	-.078	.217	<b>.566</b>	.079	.076	-.148	.078	.050
<b>FitsWork</b>	<b>.564</b>	.213	.031	.056	<b>.668</b>	-.090	.110	.018	-.064	.079
<b>FitsStyle</b>	<b>.514</b>	.240	.057	.099	<b>.682</b>	-.098	.103	-.006	-.026	.114
<b>Prestige</b>	.252	.061	.076	<b>.858</b>	.080	.003	.080	-.130	.031	-.020
<b>Profile</b>	.218	.062	.083	<b>.902</b>	.068	.036	.051	-.076	.018	-.008
<b>Status</b>	.094	.046	.018	<b>.885</b>	.064	.078	-.078	-.033	.104	.013
<b>Clear</b>	.185	<b>.601</b>	-.034	.076	<i>.413</i>	-.025	.083	.005	.053	.168
<b>EasyToGet</b>	.317	<b>.722</b>	.051	.124	.186	.043	-.063	-.001	.007	.007
<b>EasyToUse</b>	.239	<b>.842</b>	-.007	-.015	.109	.015	-.009	-.012	.010	.071
<b>EasyOperate</b>	.215	<b>.869</b>	.026	-.038	-.047	-.051	.148	-.036	.047	.039

Table 4.13 continued

Rotated Component Matrix										
	Factor									
	voluntariness	relative advantage	compatibility	image	ease of use	result demonstrability	visibility	trialability	severity of threat	susceptibility to threat
<b>TellOthers</b>	.174	.668	-.042	.102	.047	-.103	.468	.063	.059	.043
<b>CommConsequ</b>	.006	.489	.104	.146	.151	-.080	.552	-.149	.131	.028
<b>ApparentResults</b>	.179	.485	.047	.101	.275	-.056	.482	-.023	.209	.194
<b>DiffExplainBene</b>	-.094	-.073	.064	.062	-.029	-.021	<b>-.817</b>	-.017	.163	-.125
<b>SeeOthers</b>	.098	.179	-.043	.077	.227	.038	.035	-.138	-.026	<b>.792</b>
<b>NotVisable</b>	-.214	-.042	.077	.093	.060	.113	-.174	-.037	.081	<b>-.820</b>
<b>ProperlyTry</b>	.065	.160	.051	.029	.021	.050	-.039	.095	<b>.850</b>	.054
<b>PermittedToUse</b>	.042	-.014	.045	.104	-.009	.045	-.016	-.187	<b>.798</b>	-.155
<b>SecuritySevere</b>	.025	-.001	<b>.885</b>	.089	-.056	.142	-.040	.032	.074	-.018
<b>SecuritySerious</b>	.009	.024	<b>.925</b>	.006	.037	.129	.004	.019	.024	-.012
<b>SecuritySignificant</b>	-.001	.021	<b>.897</b>	.032	.023	.152	.003	-.006	.018	-.102
<b>DataWrongHands</b>	-.008	.017	.642	.069	-.012	.547	.019	.011	-.012	.032
<b>NegConLikely</b>	-.010	-.087	.264	.122	-.067	<b>.747</b>	-.185	-.001	.157	-.084
<b>NegConPoss</b>	-.030	-.015	.305	-.012	.010	<b>.830</b>	.101	-.009	-.024	-.013
Extraction Method: Principal Component Analysis.										
Rotation Method: Varimax with Kaiser Normalization.										



It is advisable to find the highest loading for a variable on any given factor and consider removing any variables that have several high loadings (Hair Jr. et al., 1998). It is difficult to obtain a specific threshold for the number of unacceptable cross loadings and Hair Jr. et al. (1998, p. 113) offer the following advice: “A variable with several high loadings is a candidate for deletion.” The proper course of action is not always clear when there are smaller issues with cross loadings (Straub, Boudreau, & Gefen, 2001).

Straub et al. (2001) report that items which do not load properly can be dropped from analysis as do Gerbing & Anderson (1988) or left in, as suggested by MacCallum & Austin (2000). Straub himself has been known to include items with cross loadings (see Karahanna et al., 1999). Some researchers report the cross loadings and leave the evaluation to the reader (Richins & Dawson, 1992). Yet others merely include the highest score for each item (Torkzadeh et al., 2002). Further, it has been suggested that variables with significant cross loadings should remain if the goal is to develop factor scores (R. Taylor, personal communication, Spring semester, 2002).

However, in the case of developing a model for the purpose of increasing the understanding of a phenomena, it might be more appropriate to have fewer cross loadings. In this way, there are fewer questions that measure more than one factor. The resulting model is then easier to explain and comprehend. This concept of dimensionality reduction can be particularly useful to reduce the complexity of a research model. In any case, the loadings were somewhat different than reported in the original research. Table 4.14 indicates the factors on which the items were reported to load in the original research (see Moore et al., 1991; Witte et al., 1996).

Table 4.14

Loadings Presented in the Original Research

Item	Factor									
	voluntariness	relative advantage	compatibility	image	ease of use	result demonstrability	visibility	trialability	severity of threat	susceptibility to threat
ProfRequire	X									
NotCompuls	X									
Wquickly		X								
ImprovQual		X								
Ejob		X								
Effective		X								
Control		X								
Compatible			X							
FitsWork			X							
FitsStyle			X							
Prestige				X						
Profile				X						
Status				X						
Clear					X					
EasyToGet					X					
EasyToUse					X					

Table 4.14 continued

Item	Factor									
	voluntariness	relative advantage	compatibility	image	ease of use	result demonstrability	visibility	trialability	severity of threat	susceptibility to threat
EasyOperate					X					
TellOthers						X				
CommConsequ						X				
ApparentResults						X				
DiffExplainBene						X				
SeeOthers							X			
NotVisable							X			
ProperlyTry								X		
PermittedToUse								X		
SecuritySevere									X	
SecuritySerious									X	
SecuritySignificant									X	
DataWrongHands										X
NegConLikely										X
NegConPoss										X

In an effort to reduce the significant cross loadings and to investigate the possibility that the newly synthesized instrument may load differently, exploratory factor

analysis (EFA) was executed. Varimax with Kaiser Normalization was used to rotate the matrix and factors with eigenvalues greater than or equal to 1.0 were retained. EFA produced seven factors with only two potential issues with cross loadings. The resulting seven factors accounted for 67.52% for the total variance. The seven factors are entitled Improvement Potential, Usage, Susceptibility and Severity of Threat, Image, Voluntariness, Visibility, and Trialability. Results are depicted in table 4.15. Cross-loadings are depicted with italics. As can be observed in table 4.15, it is a great deal less chaotic when EFA is used to uncover the underlying item relationships rather than force the relationships into ten factors as is done with CFA.

Table 4.15

## EFA Results Rotated Component Matrix

Item	Factor						
	Improvement Potential	Usage	Susceptibility and Severity of Threat	Image	Voluntariness	Visibility	Triability
ProfRequire	-.106	.015	-.032	-.040	<b>.848</b>	-.022	-.121
NotCompuls	-.341	-.059	.095	-.198	<b>.734</b>	-.077	.038
Wquickly	<b>.740</b>	.215	.048	.017	-.088	.103	-.019
ImprovQual	<b>.729</b>	.126	-.047	.200	-.330	-.089	.106
Ejob	<b>.793</b>	.190	-.011	.042	-.090	.185	.022
Effective	<b>.812</b>	.126	.013	.157	-.239	.050	.042
Control	<b>.792</b>	.100	-.003	.188	-.124	.041	.055
Compatible	<b>.570</b>	.261	-.033	.237	-.062	.123	.091
FitsWork	<b>.783</b>	.245	-.020	.074	.084	.135	-.113
FitsStyle	<b>.752</b>	.277	-.001	.114	.076	.158	-.077
Prestige	.268	.102	.076	<b>.851</b>	-.148	-.025	.009
Profile	.240	.086	.098	<b>.893</b>	-.088	-.020	.013
Status	.143	.016	.059	<b>.873</b>	-.011	-.019	.143
Clear	.411	.570	-.047	.060	.112	.147	.080
EasyToGet	.478	.573	.056	.076	.077	-.094	.098
EasyToUse	.388	<b>.698</b>	-.008	-.070	.065	-.040	.104
EasyOperate	.280	<b>.803</b>	-.008	-.095	-.019	-.060	.083
TellOthers	.192	<b>.801</b>	-.083	.089	.018	.081	-.022
CommConsequ	.043	<b>.727</b>	.059	.158	-.173	.124	-.011
ApparentResults	.258	<b>.680</b>	.021	.110	-.036	.281	.090
DiffExplainBene	.033	<b>-.428</b>	.030	.009	.130	-.369	.351
SeeOthers	.246	.156	-.017	.057	-.051	<b>.740</b>	.020
NotVisable	-.192	-.084	.115	.118	.000	<b>-.765</b>	.108
ProperlyTry	.060	.185	.070	.024	.070	.038	<b>.812</b>
PermittedToUse	-.008	.052	.064	.115	-.226	-.128	<b>.739</b>
SecuritySevere	.021	.025	<b>.844</b>	.061	.022	-.113	.004
SecuritySerious	.041	.074	<b>.872</b>	-.016	.028	-.089	-.063
SecuritySignificant	.022	.068	<b>.859</b>	.013	.000	-.166	-.062
DataWrongHands	-.009	-.002	<b>.827</b>	.066	.012	.055	.034
NegConLikely	-.038	-.227	<b>.589</b>	.130	.005	-.026	.326
NegConPoss	-.059	-.048	<b>.669</b>	.015	-.021	.138	.102

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

The result of the EFA shows there are seven major factors. The five items from the original construct of Relative Advantage and the three items from Compatibility were combined into one single construct. The constructs on which the items loaded can be seen in table 4.15. These eight items form the new construct deemed “Improvement Potential.” The original four items in the Ease of Use construct combined with the four items from Result Demonstrability to form a construct entitled “Usage.” The three factors from Severity of Threat and the three factors from Susceptibility to Threat all loaded on the same construct. These combined items are termed “Susceptibility and Severity of Threat.” There was a cross loading found in the Improvement Potential construct. The items that lead to the cross loading are .411 (Clear) and .478 (EasyToUse). Considering the issues relating to cross loadings, as discussed above, and the fact that the loadings for the primary factor .570 (Clear) and .573 (EasyToUse) are higher than their respective cross loadings, those items were left in the Improvement Potential construct. Table 4.16 depicts the resulting factor structure with the rotated component matrix.



Table 4.16 continued

	Factor						
	1	2	3	4	5	6	7
	Improvement Potential	Usage	Susceptibility and Severity of Threat	Image	Voluntariness	Visibility	Triability
NotVisable						-.765	
ProperlyTry							.812
PermittedToUse							.739
SecuritySevere			.844				
SecuritySerious			.872				
SecuritySignificant			.859				
DataWrongHands			.827				
NegConLikely			.589				
NegConPoss			.669				

Extraction Method: Principal Component Analysis.  
Rotation Method: Varimax with Kaiser Normalization.

Cronbach's alpha can be used to measure how multiple indicators in a summated scale belong together (Garson, 2005) and is the most widely used measure of consistency within a scale (Hair Jr. et al., 1998). Cronbach's alpha typically ranges from zero to one, where one indicates the highest level of reliability within a scale. Typically in social science research a Cronbach's alpha of .70 or higher is needed before the scale is considered valid, while in some cases, a Cronbach's alpha of .60 is considered adequate (Garson, 2005; Hair Jr. et al., 1998). Table 4.17 depicts the factors, items leading to the factors, and the resulting Cronbach's alpha.



Table 4.17  
Construct Reliability

<b>Construct</b>	<b>Item</b>	<b>Cronbach's alpha</b>
Improvement Potential	Wquickly ImprovQual Ejob Effective Control Compatible FitsWork FitsStyle	.919
Usage	Clear EasyToGet EasyToUse EasyOperate TellOthers CommConsequ ApparentResults DiffExplainBene	.859
Susceptibility and Severity of Threat	SecuritySevere SecuritySerious SecuritySignificant DataWrongHands NegConLikely NegConPoss	.877
Image	Prestige Profile Status	.907
Voluntariness	ProfRequire NotCompuls	.688
Visibility	SeeOthers NotVisable	.632
Trialability	ProperlyTry PermittedToUse	.620

Table 4.18 presents Pearson Correlations for the seven factors and the two dependent variables. As the table depicts, there is a significant positive correlation between the dependent variable CheckAcctNLH and Usage. The correlation is however relatively low at .102. Additionally, there is a significant negative correlation between CheckAcctNLH and SecConcern.

The table depicts somewhat more encouraging results with the second dependent variable. Specifically, there are significant negative correlations between the independent variables Improvement Potential and Visibility and the dependent variable Security Concern. However, the magnitudes are relatively small given the correlations of -.123 and -.118 respectively. Additionally, there is a significant positive correlation between Susceptibility and Severity of Threat and Security Concern (.408).

Among the independent variables, there were several significant correlations. For example, the construct of Improvement Potential had a significant positive correlated to Image, Usage, Visibility, and Trialability. Improvement Potential had a significant negative correlation with Voluntariness.

Table 4.18

## Pearson Correlations

**Correlations<sup>a</sup>**

	CheckAcct NLH	SecConcern	Vol	ImpPot	Img	Use	Vis	Trial	SSThreat
CheckAcctNLH	1	-.197**	-.068	.054	-.013	.102*	-.001	.032	-.048
		.000	.147	.249	.785	.031	.978	.504	.314
SecConcern	-.197**	1	.076	-.123**	-.013	-.049	-.118*	.073	.408**
	.000		.106	.009	.776	.294	.013	.121	.000
Vol	-.068	.076	1	-.350**	-.266**	-.095*	-.158**	-.111*	.030
	.147	.106		.000	.000	.045	.001	.018	.526
ImpPot	.054	-.123**	-.350**	1	.374**	.402**	.342**	.101*	-.012
	.249	.009	.000		.000	.000	.000	.032	.806
Img	-.013	-.013	-.266**	.374**	1	.078	.026	.152**	.122**
	.785	.776	.000	.000		.099	.581	.001	.010
Use	.102*	-.049	-.095*	.402**	.078	1	.329**	-.006	-.054
	.031	.294	.045	.000	.099		.000	.899	.253
Vis	-.001	-.118*	-.158**	.342**	.026	.329**	1	-.090	-.127**
	.978	.013	.001	.000	.581	.000		.057	.007
Trial	.032	.073	-.111*	.101*	.152**	-.006	-.090	1	.143**
	.504	.121	.018	.032	.001	.899	.057		.002
SSThreat	-.048	.408**	.030	-.012	.122**	-.054	-.127**	.143**	1
	.314	.000	.526	.806	.010	.253	.007	.002	

\*\* Correlation is significant at the 0.01 level (2-tailed).

\* Correlation is significant at the 0.05 level (2-tailed).

a. Listwise N=451

As can be seen in table 4.16, the items of Wquickly, ImprovQual, Ejob, Effective, Control, Compatible, FitsWork, and FitsStyle, with the factor loadings of .740, .729, .793, .812, .792, .570, .783, and .752 respectively, form the construct of Improvement Potential. Taken together, these items attempt to capture the essence of how wireless can be used to improve some aspect of work. As can be seen in table 4.17, the Cronbach's alpha is very high (.919). The second factor, Usage, is composed of the items Clear, EasyToGet, EasyToUse, EasyOperate, TellOthers, CommConsequ, ApparentResults, and DiffExplainBene. These items attempt to assess issues regarding the potential use and benefits of using wireless. Cronbach's alpha is an acceptable .859 for this factor.

Susceptibility and Severity of threat contains six items. Image contains three items, while Voluntariness, Visibility, and Trialability each contain two items. The loadings can be viewed in table 4.16, while the actual questions that form the constructs can be seen in appendix D. For comparison purposes, the loadings in the original studies can be seen in table 4.14.

During the final factor analysis procedure, the factor scores were saved as variables. This procedure of creating a summated scale is accomplished by synthesizing several variables into a single factor, a composite measure. The resulting factor scores have two specific benefits (Hair Jr. et al., 1998). The first relates to the reduction in measurement error, due to the reduction of the coefficient of variation of the sum (and average) compared with that of a single variable, which may have specific errors because of the difficulty of individuals in accurately understanding and answering a specific question or data entry errors. The second benefit is that a composite measure provides a richer description of an environmental phenomenon while maintaining parsimony when the factor scores are used in other multivariate techniques. Taken together, these two benefits can serve to increase the validity and actionability of the results (Grapentine, 1995).

Although he is a supporter of Innovation Diffusion Theory, R. Panko recently criticized the Theory for treating adoption as a binary on/off decision (personal communication, September 5, 2005). Panko went on to state that it is far more interesting to study the level of adoption (i.e. light, medium, and heavy adopters). Mindful of this fact, this study utilized a multichotomous or multilevel dependent variable. One of the

dependent variables was designed to measure the degree to which users might use wireless technologies in light of security concerns when given a task where security is of relative importance.

### Logistic Regression

SPSS was used to determine if the main effects and interaction effects were significant in the context of a logistic regression model. The survey instrument included a scenario whereby respondents were given a fictitious lump sum of money that was to be invested in the stock market. After reading the scenario, respondents were to indicate their willingness to use a wireless network to manage their investments. Respondents were also asked to indicate their concern for security on a one to ten scale. Figure 4.3 and 4.4 depict histograms that detail the responses for the dependent variables.

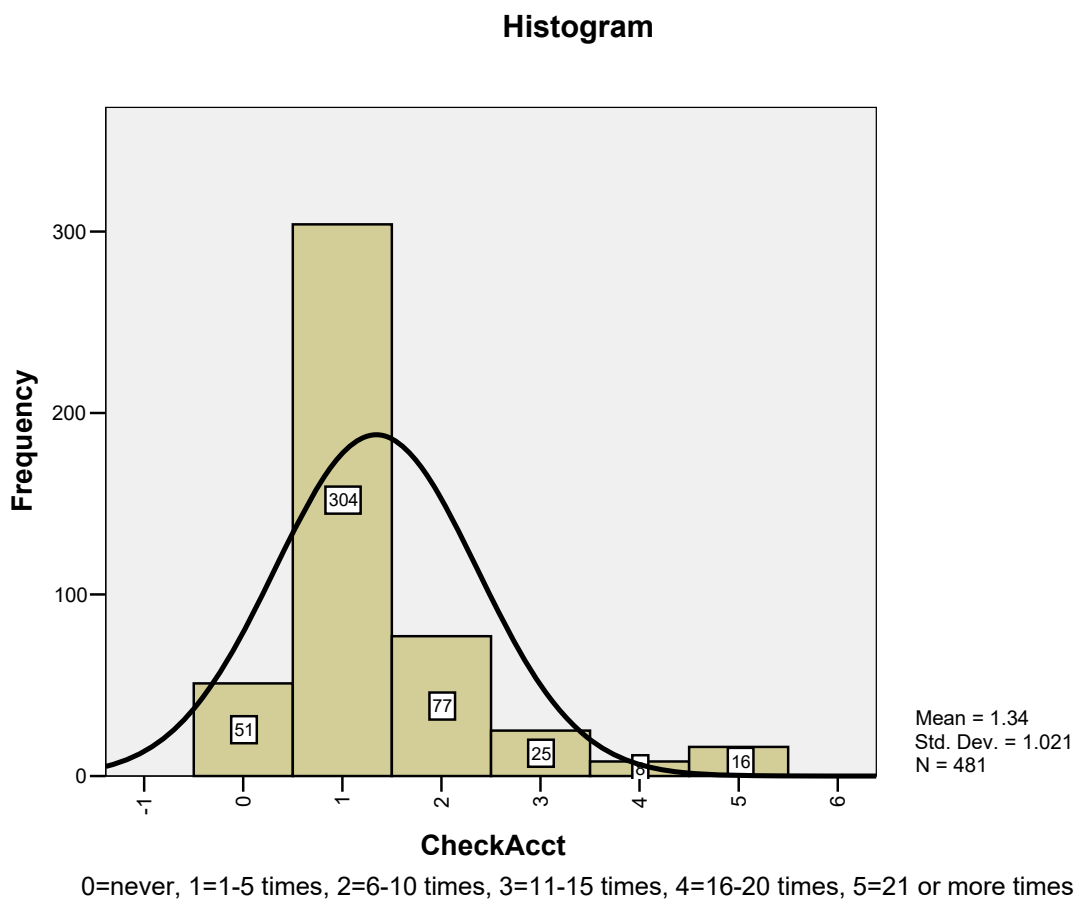


Figure 4.3: Dependent Variable Histogram (Check Account)

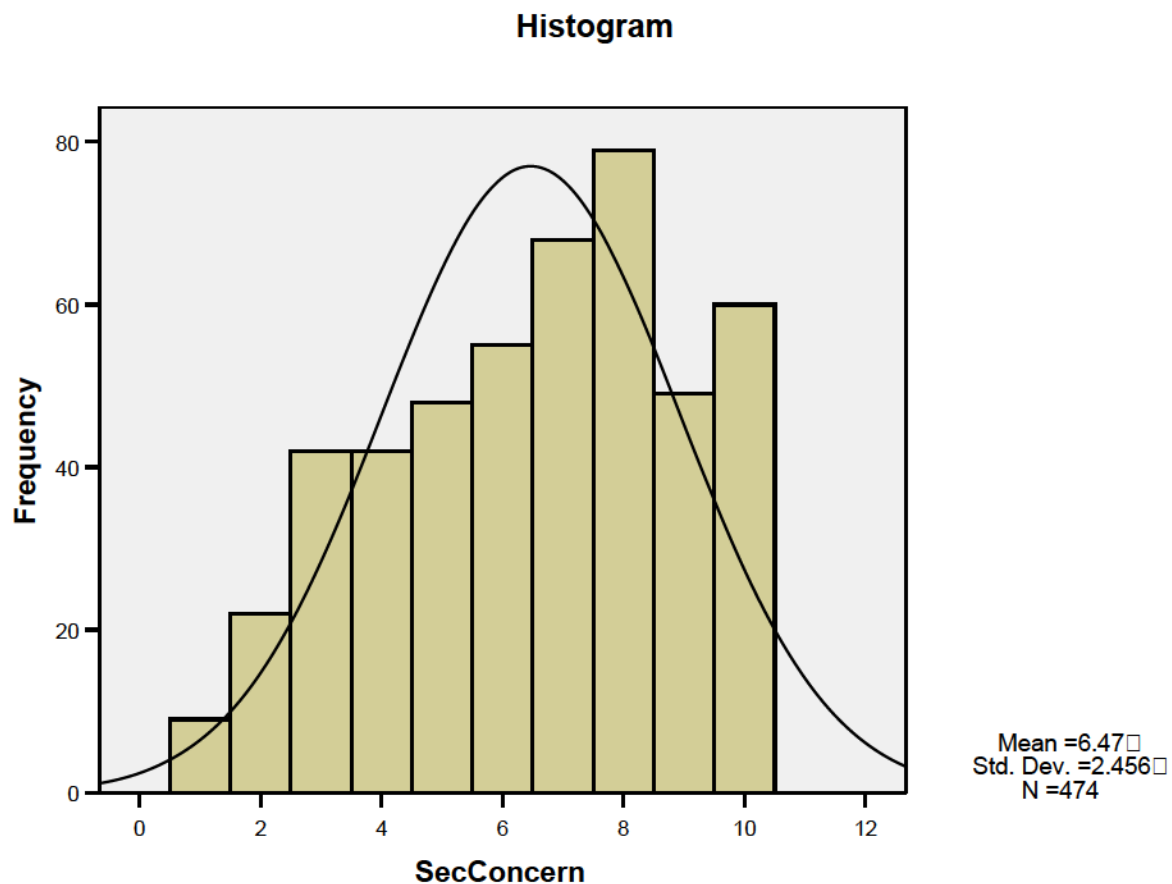


Figure 4.4: Dependent Variable Histogram (Level of Concern)

When there are several sparse categories, a more meaningful model may be obtained by aggregating sparse categories (J. Sullivan, personal communication, September 27, 2005). The dominant category, with 304 respondents, was retained. The never category was retained to represent non-users. Because the four higher use categories account for a combined 26.2% of the responses, those four categories were

collapsed into one to represent heavy users. The resulting categories then were non-users, light users, and heavy users. Table 4.19 depicts the resulting categories.

Table 4.19  
Compressed Dependent Variables Categories and Frequencies

Category	Number of Respondents	Percent
Non-users (original category = Never)	51	10.6
Light Users (original category = 1-5)	304	63.2
Heavy Users (original categories = 6-10, 11-15, 16-20, and 21 or more)	126	26.2
Total	481	100

The results of multinomial logistic regression using the three levels of non-users, light users, and heavy users, reveal one significant construct (Usage). An examination of Table 4.20 reveals the significant variable.



Table 4.20

## Parameter Estimates of Multinomial Logistic Regression

Check-AcctNLH		B	Std. Error	Wald	df	Sig.	Exp(B)
0	Intercept	-0.943	0.175	29.061	1	0.000	
	F1 Imp Pot	-0.042	0.169	0.063	1	0.802	0.959
	F2 Use	-0.341	0.169	4.097	1	0.043	0.711
	F3 SS Threat	0.134	0.171	0.612	1	0.434	1.143
	F4 Img	0.129	0.167	0.596	1	0.440	1.138
	F5 Vol	0.215	0.175	1.507	1	0.220	1.240
	F6 Vis	-0.169	0.168	1.015	1	0.314	0.844
	F7 Trial	-0.106	0.167	0.400	1	0.527	0.900
1	Intercept	0.903	0.108	69.732	1	0.000	
	F1 Imp Pot	0.001	0.107	0.000	1	0.994	1.001
	<b>F2 Use</b>	<b>-0.290</b>	<b>0.111</b>	<b>6.838</b>	<b>1</b>	<b>0.009</b>	<b>0.749</b>
	F3 SS Threat	0.019	0.106	0.032	1	0.859	1.019
	F4 Img	-0.025	0.108	0.055	1	0.815	0.975
	F5 Vol	0.030	0.106	0.081	1	0.776	1.031
	F6 Vis	0.122	0.109	1.269	1	0.260	1.130
	F7 Trial	-0.019	0.107	0.030	1	0.862	0.982

This model, with one of seven significant constructs, was then further examined for its ability to accurately predict the level of use. Table 4.21 presents a classification matrix for the data. As can be seen in table 4.21, the model correctly predicts one of the 126 heavy users while predicting the other 125 as light users. Thus this particular model achieves an overall accuracy of 63.4%, while a naïve model that predicts all respondents to fit in the light user category would achieve an overall accuracy of 63.2%.

Table 4.21

Classification Matrix for Model with Non, Light, and Heavy Users

Classification				
Observed	Predicted			Percent Correct
	0	1	2	
0	0	51	0	.0%
1	0	304	0	100.0%
2	0	125	1	.8%
Overall Percentage	.0%	99.8%	.2%	63.4%

Even though there was one significant construct, a .2% increase in overall model accuracy was not impressive. Because of the limited results of the multinomial logistic regression procedure, a binary logistic regression model was explored. The dependent variable was partitioned into non-users and users. Table 4.22 depicts the resulting categories.

Table 4.22

Binary Dependent Variables Categories and Frequencies

Category	Number of Respondents	Percent
Non-users (original Never)	51	10.6
Users (all other responses)	430	89.4
Total	481	100

The resulting model was able to predict the correct category 89.4% of the time. Unfortunately, 89.4% corresponds directly to the percentage of users of wireless

technologies. As table 4.23 shows, none of the seven constructs were significant in the model.

Table 4.23  
Model for Binary Dependent Variable

Variables not in the Equation			Score	df	Sig.
Step	Variables	F1 Imp Pot	.075	1	.785
0		F2 Use	.783	1	.376
		F3 SS Threat	.627	1	.429
		F4 Img	.803	1	.370
		F5 Vol	1.520	1	.218
		F6 Vis	2.855	1	.091
		F7 Trial	.371	1	.542
	Overall Statistics		7.033	7	.425

As a result of none of the seven factor scores being significant, where the p-value  $< .05$ , the model simply predicts that everyone is a user. While the resulting accuracy is relatively high (89.4%), the model is not very useful if none of the predictors is significant. Table 4.24 details the overall accuracy of the model. Similar to the predictions of the naïve model, all respondents are predicted to be members of the most populous category.

Table 4.24  
Model Prediction Accuracy

Classification Table<sup>a,b</sup>

Observed			Predicted		Percentage Correct
			CheckAcctYN		
			0	1	
Step 0	CheckAcctYN	0	0	51	.0
		1	0	430	100.0
	Overall Percentage				89.4

a. Constant is included in the model.

b. The cut value is .500

#### Evaluation of Research Hypotheses

Because the exploratory factor analysis found seven factors as compared to the original ten, the hypotheses are slightly different than proposed in chapter three. There were three combinations that lead to the reduced number of constructs. The first of the combinations occurred with the five items in the original construct Relative Advantage and the three items in the original construct Compatibility. The resulting construct was termed “Improvement Potential.” The second combination occurred when the original four items in Ease of Use were merged with the four items from Result Demonstrability to form the construct of “Usage.” The third combination occurred with the three items from Severity of Threat and the items from Susceptibility to Threat. The resulting construct was termed “Susceptibility and Severity of Threat.” The revised hypotheses are presented in Table 4.25.

Table 4.25

## Revised Hypotheses

<b>Hypothesis</b>	<b>Result</b>
H <sub>1</sub> : Voluntariness will have a significant positive effect on user intention to use the wireless network.	Not supported
H <sub>2</sub> : Improvement potential will have a significant positive effect on user intention to use the wireless network	Not supported
H <sub>3</sub> : Image will have a significant positive effect on user intention to use the wireless network.	Not supported
H <sub>4</sub> : Usage will have a significant positive effect on user intention to use the wireless network.	Not supported
H <sub>5</sub> : Visibility will have a significant positive effect on user intention to use the wireless network.	Not supported
H <sub>6</sub> : Trialability will have a significant positive effect on user intention to use the wireless network.	Not supported
H <sub>7</sub> : Susceptibility and Severity of Threat will have a significant negative effect on user intention to use the wireless network.	Not supported
H <sub>8</sub> : There are interaction effects between Susceptibility and Severity of Threat and any of the other constructs.	Not Supported

### Model Construction with MSU-only Data

Due to the non significant results of the logistic regression model using the full data set, other models were considered. In seeking a better model, two additional sets of models were constructed and evaluated. The first set of models was constructed based on data from MSU. The rationale is that there may have been a fundamental difference in the manner in which students from a university that requires laptops with wireless capabilities answered the questionnaire compared to the way students who attend a university that does not require laptops might answer the questionnaire.

In total, there were 273 useable responses from MSU. A factor analysis of this data produced significant results with a Kaiser-Meyer-Olkin Measure of Sampling Adequacy at .845 (significance of .000). Varimax with Kaiser Normalization was used to rotate the matrix and factors with eigenvalues greater than or equal to 1.0 were retained. The analysis revealed slightly different results compared to the analysis of the full data set. The MSU-only data identified eight factors as compared to seven factors when the full data set was analyzed. The resulting eight factors explained 71.44% of the total variance. The rotated component matrix looked remarkably similar to that of the full data set.

There were only two significant cross loadings in both the full and MSU-only data. The loadings were remarkably similar to the loadings observed in the full data set. In fact, the 31 items loaded on the same constructs with two exceptions. The first is that DiffExplainBene became part of the Visibility construct in the MSU-only analysis. The second difference is found in the security related items. Analysis of the full data set

revealed that the six items (SecuritySevere, SecuritySerious, SecuritySignificant, DataWrongHands, NegConLikely, and NegConPoss) all loaded together to form the construct termed Susceptibility and Severity of Threat. Comparatively, in the MSU data, SecuritySevere, SecuritySerious, SecuritySignificant, and DataWrongHands loaded together, as did DataWrongHands, NegConLikely, and NegConPoss. A cross loading was observed with the item DataWrongHands.

Factor scores were then created and saved for each of the eight constructs identified in the factor analysis. In turn, those factor scores were used in a binary logistic regression procedure. One of the eight variables (Trialability) was significant in this analysis. Table 4.26 presents the significance levels of each of the eight constructs.

Table 4.26

## Significance Level of Constructs for MSU Data for Binary Logistic Regression

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1	F1 Imp Pot	-.081	.215	.142	1	.706	.922
	F2 Use	.097	.218	.196	1	.658	1.101
	F3 Sev Threat	-.204	.218	.873	1	.350	.816
	F4 lmg	-.135	.214	.396	1	.529	.874
	F5 Vol	-.392	.243	2.594	1	.107	.676
	F6 Vis	.291	.210	1.920	1	.166	1.338
	F7 Sus Threat	-.204	.216	.888	1	.346	.816
	F8 Trial	.527	.217	5.875	1	.015	1.694
	Constant	2.489	.248	100.440	1	.000	12.053

Unfortunately, the model simply predicts everyone to be a user, as does the naïve model. Accordingly, the model is not useful in attempting to predict usage behavior.

Table 4.27 depicts the results of the model. By simply predicting everyone as a user, the model achieves 90.5% accuracy. Similar to the results found using the full data set, these results appear to suggest that because the percentage of users is so high, it is difficult to distinguish users from non-users.

Table 4.27

Predicted Results for MSU-only Data Using Binomial Logistic Regression

**Classification Table<sup>a,b</sup>**

Observed			Predicted		Percentage Correct
			CheckAcctYN		
			0	1	
Step 0	CheckAcctYN	0	0	26	.0
		1	0	247	100.0
	Overall Percentage				90.5

a. Constant is included in the model.

b. The cut value is .500

Further analysis of the MSU data was conducted in an effort to increase the effectiveness of the model. In the next model, the dependent variable included non-users, light users, and heavy users. Multinomial logistic regression was used to regress the three category dependent variable on the eight factors identified in factor analysis. The construct of Usage was the sole significant construct in the model. Table 4.28 depicts the significant variable in this model.



Table 4.28

Significance Level of the Constructs for MSU-only Data for Multinomial  
Logistic Regression

**Parameter Estimates**

CheckAcct NLH <sup>a</sup>		B	Std. Error	Wald	df	Sig.
0	Intercept	-1.189	.271	19.245	1	.000
	F1 Imp Pot	.168	.240	.489	1	.484
	F2 Use	-.381	.248	2.361	1	.124
	F3 Sev Threat	.060	.242	.061	1	.805
	F4 Img	.247	.239	1.070	1	.301
	F5 Vol	.363	.264	1.889	1	.169
	F6 Vis	-.208	.234	.795	1	.373
	F7 Sus Threat	.094	.241	.152	1	.697
	F8 Trial	-.572	.241	5.645	1	.018
1	Intercept	.942	.147	40.919	1	.000
	F1 Imp Pot	.134	.146	.843	1	.359
	F2 Use	-.407	.152	7.171	1	.007
	F3 Sev Threat	-.205	.145	1.993	1	.158
	F4 Img	.157	.146	1.162	1	.281
	F5 Vol	-.040	.144	.076	1	.783
	F6 Vis	.119	.144	.681	1	.409
	F7 Sus Threat	-.148	.146	1.033	1	.310
	F8 Trial	-.071	.146	.241	1	.624

a. The reference category is: 2.

Unfortunately, the model demonstrates results only slightly better than the naïve model. Accordingly, the model is not useful in attempting to predict usage behavior. Table 4.29 depicts the results of the model. By simply predicting everyone as a user, the naïve model achieves 64.1% accuracy, while the model under consideration improves the accuracy rate to 64.8%. The resulting .7% improvement is encouraging, but additional research is needed in an effort to discover a model with more predictive value.

Table 4.29

Predicted Results for MSU-only Data Using Multinomial Logistic Regression

**Classification**

Observed	Predicted			Percent Correct
	0	1	2	
0	1	25	0	3.8%
1	1	169	5	96.6%
2	0	65	7	9.7%
Overall Percentage	.7%	94.9%	4.4%	64.8%

**Model Construction with WSU-only Data**

The second set of models constructed and evaluated was based on WSU data only. In total, there were 208 useable responses from WSU. A factor analysis of this data produced significant results with a Kaiser-Meyer-Olkin Measure of Sampling Adequacy at .847 (significance of .000). Varimax with Kaiser Normalization was used to rotate the matrix and factors with eigenvalues greater than or equal to 1.0 were retained. The resulting seven factors were able to explain 68.04% of the total variance.

The analysis revealed slightly different results compared to the analysis of the full data set. The analysis using WSU-only data identified seven factors as did the analysis of the full data set. The rotated component matrix looked remarkably similar to that of the full data set. There were only two significant cross loadings in the full data set, and there were four cross loadings in the WSU-only data.

The items loaded on the same constructs with few exceptions. The first is that NotCompuls cross loaded on the Voluntariness and Improvement Potential constructs in the WSU-only analysis. Also SeeOthers became part of the Improvement Potential construct. CommConsequ and ApparentResults cross loaded on the constructs of Usage and Visibility. Another difference is found in the Visibility construct. DiffExplainBene was added to Visibility construct.

Factor scores were then created and saved for each of the seven constructs identified in factor analysis. In turn, those factor scores were used in a binary logistic regression procedure. Of the seven variables none were significant in this analysis. Table 4.30 presents the significance level of each of the constructs.

Table 4.30

Significance Level of the Constructs for WSU-only Data for Binary Logistic Regression

Variables not in the Equation			Score	df	Sig.
Step	Variables	F1 Imp Pot	1.830	1	.176
0		F2 SS Threats	.194	1	.660
		F3 Use	.000	1	.993
		F4 Img	.562	1	.454
		F5 Vis	1.800	1	.180
		F6 Trial	1.012	1	.314
		F7 Vol	.061	1	.805
	Overall Statistics		5.459	7	.604

Regrettably, the model produces the same results as the naïve model. As a result this model is not useful in predicting usage behavior. Table 4.31 depicts the results of the

model. By simply predicting everyone as a user, the naïve model achieves 88.0% accuracy as does the model under consideration. Next, a model will be constructed using multinomial logistic regression using the WSU data.

Table 4.31

Predicted Results for WSU-only Data Using Binomial Logistic Regression

**Classification Table<sup>a</sup>**

Observed			Predicted		Percentage Correct
			CheckAcctYN		
			0	1	
Step 1	CheckAcctYN	0	0	25	.0
		1	0	183	100.0
Overall Percentage					88.0

a. The cut value is .500

Further analysis of the WSU data was conducted in an effort to discover an effective model. In the next model, the dependent variable included non-users, light users, and heavy users. Multinomial logistic regression was used to regress the three category dependent variable on the seven factors identified in factor analysis. As was the case with the previous model, none of the predictor variables were significant. Table 4.32 depicts the significant level of the variables.

Table 4.32

Significance Level of the Constructs for WSU Data for Multinomial Logistic Regression

Parameter Estimates						
CheckAcctNLH <sup>a</sup>		B	Std. Error	Wald	df	Sig.
0	Intercept	-.799	.263	9.219	1	.002
	F1 Imp Pot	-.327	.244	1.796	1	.180
	F2 SS Threats	.302	.256	1.393	1	.238
	F3 Use	-.134	.253	.280	1	.597
	F4 Img	-.056	.255	.049	1	.825
	F5 Vis	-.232	.257	.814	1	.367
	F6 Trial	.258	.245	1.105	1	.293
	F7 Vol	.128	.251	.260	1	.610
1	Intercept	.926	.171	29.449	1	.000
	F1 Imp Pot	-.043	.172	.063	1	.801
	F2 SS Threats	.305	.170	3.234	1	.072
	F3 Use	-.177	.171	1.070	1	.301
	F4 Img	-.305	.175	3.048	1	.081
	F5 Vis	.087	.175	.250	1	.617
	F6 Trial	.067	.167	.160	1	.689
	F7 Vol	.252	.169	2.207	1	.137

a. The reference category is: 2.

Unfortunately, the model is not significant (.332). Accordingly, the model is not useful in attempting to predict usage behavior. Table 4.33 depicts the results of the model. By simply predicting everyone as a light user, the naïve model achieves 62% accuracy; while the model under consideration actually decreases that accuracy to 61.1%. Even though this model is not significant, a classification matrix was included in this description so a consistent discussion for all the models could be presented. The results of this model are of course discouraging. Given these results, more research is needed.

Table 4.33

Classification Matrix for Multinomial Logistic Regression Using WSU Data

<b>Classification</b>				
Observed	Predicted			Percent Correct
	0	1	2	
0	0	25	0	.0%
1	0	124	5	96.1%
2	0	51	3	5.6%
Overall Percentage	.0%	96.2%	3.8%	61.1%

Using the full, MSU-only, and WSU-only data sets, a total of six models were considered for analysis. Three of the models use the multinomial logistic regression technique, and the remaining three used binomial logistic regression. Although there were some significant findings with some of the models, a better model was pursued. Table 4.34 details the specific results of the seven models.

Table 4.34

## Summary of Results

Data set	Dependent Variable	Results
Full n=481	Collapsed into 3 categories (non, low, & high users)	One significant construct
	Collapsed into 2 categories (non-users & users)	One significant construct
MSU-only n=273	Collapsed into 3 categories (non, low, & high users)	One significant construct
	Collapsed into 2 categories (non-users & users)	One significant construct
WSU-only n=208	Collapsed into 3 categories (non, low, & high users)	One significant construct
	Collapsed into 2 categories (non-users & users)	No significant constructs

## Multiple Regression Analysis

The results in the summary table above are somewhat disappointing. Therefore, another model was sought. In the quest to find a better model to fit the full data set, the other dependent variable was utilized. The question that leads to the first dependent variable was, “If you wanted to check your account frequently how many times a day would you use the convenient but possibly risky wireless network?” The response categories for this question were (Never, 1-5, 6-10, 11-15, 16-20, and 21 or more). The question that leads to the second dependent variable was, “On a scale from 1 to 10, how concerned would you be regarding security? (1 is low – 10 is high).” The response possibilities were (1 2 3 4 5 6 7 8 9 10).

The data obtained from this second question is scale data which can be appropriate for multiple regression analysis. A multiple regression was run with SPSS 14.0 using stepwise entry for the constructs. Cases with missing data were excluded listwise in this analysis. Twelve respondents did not provide a response for this dependent variable. There were not any cases with missing factor scores. The exclusion of those 12 cases left a total of 469 cases in the analysis.

The stepwise regression procedure identified three iterations of the model. Accordingly, the final model has three significant constructs. The model was significant with an F of 33.744 and a significance level of .000. See table 4.35 for details.

Table 4.35

## ANOVA Table for Model

<b>ANOVA</b>					
	Sum of Squares	df		F	Sig.
Regression	493.299	3	164.433	33.744	.000
Residual	2265.938	465	4.873		
Total	2759.237	468			

Due to the fact that this model was significant, further analysis is prudent. The next step was to check for interaction effects with the security construct and the other constructs. To do so, interaction terms were created. In total, six new variables were created. Those six variables were derived by taking the factor score for Susceptibility and Severity of Threat and separately multiplying it by the other six constructs. The



resulting variables were termed secXip, secXuf, secXi, secXvol, secXvis, and secXt. These variables were derived from taking Susceptibility and Severity of Threat multiplied by Improvement Potential, Usage, Image, Voluntariness, Visibility, and Trialability, respectively.

With a significant model and the interaction terms created, the next step was to run a new model to assess the significance of the model in light of the interaction terms. The resulting model is significant (.000) with an F of 33.744. Table 4.36 shows the ANOVA table produced by the stepwise regression procedure.

Table 4.36

## ANOVA Table for Model with Interaction Terms

<b>ANOVA</b>					
	Sum of Squares	df		F	Sig.
Regression	493.299	3	164.433	33.744	.000
Residual	2265.938	465	4.873		
Total	2759.237	468			

Model three includes three significant variables. Those variables are Security Concerns, Improvement Potential, and Visibility. It also should be noted that a fourth variable, one of the interaction terms, Security Concerns multiplied by Improvement potential would have been the next construct to enter the model. This variable has a significance level of .053 (at .053 or higher it would have entered); while the next closest variable was the interaction term of Security Concerns multiplied by Image with a significance level of .263. Table 4.37 provides further details.

Table 4.37  
Constructs in the Model

**Coefficients<sup>a</sup>**

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	6.503	.102		63.794	.000
F3 SS Threat	.964	.102	.399	9.491	.000
F1 Imp Pot	-.264	.101	-.109	-2.600	.010
F6 Vis	-.212	.102	-.087	-2.081	.038

a. Dependent Variable: SecConcern

As can be seen in table 4.38, the model is able to account for 17.3% of the variation in the dependent variable. Although a higher percentage of course is desirable, this is a good starting place in the development of a model to assess adoption behavior in light of security concerns. The significant predictors of Susceptibility and Severity of Threat, Improvement Potential, and Visibility will be discussed in detail later in this chapter.

Table 4.38

## Model Summary

**Model Summary<sup>d</sup>**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
3	.423 <sup>c</sup>	.179	.173	2.207

c. Predictors: (Constant), F3 SS Threat, F1 Imp Pot, F6 Vis

d. Dependent Variable: SecConcern

## Evaluation of Research Hypotheses in the Final Model

Because the factor analysis found only seven factors as compared to the original ten, the hypotheses are slightly different than proposed in chapter three. The five items in the original construct of Relative Advantage were combined with the three items of Compatibility. The resulting construct was termed “Improvement Potential.” The original four items in Ease of Use were merged with the four items from Result Demonstrability to form the construct of “Usage.” A third combination occurred with the three items from Severity of Threat and the items from Susceptibility to Threat. The resulting construct was termed “Susceptibility and Severity of Threat.” Because of the aforementioned combinations, there are now seven research hypothesis that will be examined. The revised hypotheses and the result in the final model are presented in Table 4.39.

Table 4.39

## Revised Hypotheses for the Final Model

Hypothesis	Result
H <sub>1</sub> : Voluntariness will have a significant negative effect on level of security concern when using wireless for sensitive transactions.	Not supported
H <sub>2</sub> : Improvement potential will have a significant negative effect on level of security concern when using wireless for sensitive transactions	<b>Supported</b>
H <sub>3</sub> : Image will have a significant negative effect on level of security concern when using wireless for sensitive transactions.	Not supported
H <sub>4</sub> : Usage will have a significant negative effect on level of security concern when using wireless for sensitive transactions.	Not supported
H <sub>5</sub> : Visibility will have a significant negative effect on level of security concern when using wireless for sensitive transactions.	<b>Supported</b>
H <sub>6</sub> : Trialability will have a significant negative effect on level of security concern when using wireless for sensitive transactions.	Not supported
H <sub>7</sub> : Susceptibility and Severity of Threat will have a significant positive effect on level of security concern when using wireless for sensitive transactions.	<b>Supported</b>
H <sub>8</sub> : There are interaction effects between Susceptibility and Severity of Threat and any of the other constructs.	Not supported

Susceptibility and Severity of Threat can be thought of as one's risk of experiencing a threat and the importance or magnitude of the threat should it materialize (Witte et al., 1996). It stands to reason if there are threats inherent to a given innovation; users are likely to be somewhat reluctant to adopt that innovation, particularly when they perceive a level of susceptibility to that threat. Further, if one perceives the susceptibility and severity of threats to be high, the potential for the threats will likely increase the level of concern when using that innovation for a sensitive transaction.

As expected, the construct of Susceptibility and Severity of Threat has a significant positive impact on the level of concern for an innovation used for sensitive transactions. As might be expected, higher summated scores in the construct of Susceptibility and Severity of Threat effectively increase the level of concern. Accordingly, respondents who perceived the level of Susceptibility and Severity of Threat to be relatively high then exhibited a relatively high level of concern when considering wireless use for sensitive transactions. Unfortunately, there is cause for concern in today's computing paradigm. As S. Kristiansen stated, all connected devices have inherent security issues (personal communication, September 21, 2005).

The construct of Improvement Potential is formed by the items in the original perceived characteristics of innovating study (Moore et al., 1991) and from the constructs of Relative Advantage and Compatibility. Relative Advantage is the degree to which an innovation is perceived as being better than its precursor. Compatibility can be thought of as the degree to which an innovation is perceived as being consistent with the existing values, needs, and past experiences of potential adopters. Taken together, the eight

individual items from the original constructs of Relative Advantage and Compatibility form the construct of Improvement Potential.

Ceteris paribus, a potential adopter is likely to adopt an innovation if it promises to provide potential for the user to improve the level of performance (Lee, 2004).

Wireless can provide an increased level of mobility which is advantageous to many users. If an innovation has the potential to improve ones' performance while maintaining a level of compatibility with existing technologies it is likely to assist in the diffusion of that innovation (Hardgrave et al., 2003; Kaefer et al., 2004).

Potential adopters of innovations are likely to want that innovation to improve their productivity while not creating a great deal of conflict with existing innovations that they already use. P. Thorson commented that the convenience afforded by the mobility of wireless and the fact that users can be always connected, offers much potential to increase productivity in comparison to wired connections (personal communication, August 29, 2005). The users of wireless technologies stand to benefit from the convenience of wireless but need to arrive at a balance between functionality and security.

Improvement Potential was found to be a significant predictor of users' attitude toward security concerns for using wireless in sensitive transactions. As might be expected, the higher summated scores in the construct of Improvement Potential effectively reduce the level of concern. Put in another way, if users are seeking to resolve the level of risk with the level of reward, those who are likely to consider wireless to hold

a great deal of promise in regard to improving their computing milieu are less concerned about security of wireless and more concerned about its functionality.

Visibility refers to the level of observed use in the organization. Highly visible innovations are not only used frequently in an organization but might even emerge as part of that organization's culture. For instance, using wireless data access on a college campus might evolve as a status quo. If this becomes the case, it would affect a potential adopter's attitude toward an innovation. As S. Kristiansen stated wireless is something for which students no longer possess a wow factor, rather they just expect it to work because it is now a part of the culture at WSU (personal communication, September 21, 2005). Further as D. Gresham commented, everywhere you go [at WSU], the library, the student union, hallways, even outside underneath a tree, students have open laptops with them and you just know they are chatting with friends or surfing the Internet and not working on a report due for a class (personal communication, October 7, 2005).

As expected, the construct of Visibility has a significant negative impact on the level of concern for an innovation used for sensitive transactions. Users who perceive the level of visibility to be high for a given innovation are likely to consider it as safe if for no other reason than others are using it. Consequently, the more an innovation is seen as used by others, the lower the level of concern for security.

### Synthesis of Case Study and Survey Results

The adoption of wireless technologies by end users can be thought of as a two stage contingent adoption decision. The first stage involves administrators, network managers, or other decision makers choosing to adopt wireless and then deploying wireless access points for users. The second stage occurs with the potential end user deciding to utilize wireless technology. Figure 4.5 depicts the contingent adoption decision. Because of the nature of this contingent adoption decision, members from each group must adopt before wireless technology is actually used. It then becomes important to consider both groups in a thorough analysis of wireless adoption.

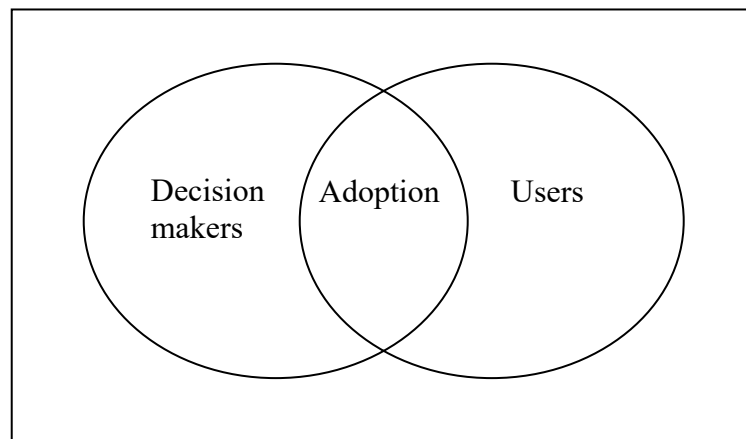


Figure 4.5: The Contingent Adoption Decision

In addition to the seven personal interviews, an effort was made to seek the thoughts of other IT professionals regarding wireless security. To that end, IT professionals were asked to complete the survey that was given to end users. IT



professionals were asked to complete the instrument from their perspective as IT professionals. In total, 30 IT professionals provided their opinions.

As might be expected, the IT professionals were a bit more concerned regarding security than were typical end users. This increased concern is likely a function of their professional positions and general knowledge of wireless security issues. So, even though heavy end users might be more susceptible to security problems, they do not have the responsibility for the secure environment for others. When asked to rate their concern about security on a scale from one to 10, IT professionals reported a mean concern of 7.56, whereas users reported a mean concern of 6.51. This difference is statistically significant at the .05 level. Table 4.40 depicts a t-test of security concern between IT professionals and end users.

Table 4.40

## T-tests for Security Concern

t-Test: Two-Sample Assuming Unequal Variances

	<i>Sec con user</i>	<i>Sec con IT pro</i>
Mean	6.505	7.556
Variance	5.896	4.718
Observations	469	27
Hypothesized Mean Difference	0	
df	30	
t Stat	-2.426	
P(T<=t) two-tail	0.021	
t Critical two-tail	2.042	

Respondents were asked to consider all factors and indicate their preference between wired and wireless networks. Of the 21 IT professionals who were able to make a choice between wired and wireless, 16 choose wired as their preferred network. Of those 16, fully half, made specific note of security issues with wireless as a primary reason they preferred wired.

The aforementioned finding is possibly because network managers are likely more cognizant of the potential security threats and they are typically charged with the mitigation of those threats. IT professionals then appear to absorb the brunt of the security issues and provide users a certain comfort level in which they feel relatively secure in their use of wireless technologies.

Individual t-tests were conducted in an effort to compare end-user and IT professional perceptions of the six items that form the Susceptibility and Severity of Threat construct. Table 4.41 details the results of those t-tests. There were no significant differences identified between end-user and IT professionals' perceptions of the six items that formed the Susceptibility and Severity of Threat construct. However, these tests do not take depth of security awareness into consideration. It is therefore possible that the typical end user is simply less aware of many possible security threats and therefore less concerned than IT professionals.

Table 4.41

## Individual t-test Results

## Independent Samples Test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
SecuritySevere	Equal variances assumed	-.153	506	.878	-.044	.289
	Equal variances not assumed	-.161	30.624	.873	-.044	.275
SecuritySerious	Equal variances assumed	-.526	506	.599	-.156	.297
	Equal variances not assumed	-.542	30.466	.592	-.156	.288
SecuritySignifican	Equal variances assumed	-.732	507	.464	-.209	.285
	Equal variances not assumed	-.689	29.804	.496	-.209	.303
DataWrongHands	Equal variances assumed	.606	506	.545	.173	.285
	Equal variances not assumed	.541	29.492	.593	.173	.319
NegConLikely	Equal variances assumed	1.701	508	.089	.450	.264
	Equal variances not assumed	1.947	31.402	.061	.450	.231
NegConPoss	Equal variances assumed	1.383	508	.167	.390	.282
	Equal variances not assumed	1.269	29.645	.214	.390	.307

In terms of network preference, IT professionals were more likely to prefer a wired network. Specifically, 76.19% of IT professionals reported that, all factors considered, they prefer to use wired networks as opposed to wireless networks. Different results were observed in the sample of student users; fewer than half (44.86%) reported

that they preferred wired over wireless networks. This may be due to the supposition that wireless is inherently insecure. While it is possible that IT professionals are partial to wired networks for their relatively high throughput potential, when asked why they chose the wired network, eight IT professionals specifically mentioned concern for security as at least part of the reason.

## CHAPTER V

### DISCUSSION AND SUMMARY

Chapter five presents a summary of the findings and their corresponding limitations. Directions for future research are also discussed. The chapter concludes with a discussion of contributions of the survey and case study, and for results that were only identified after a synthesis of techniques. Interviews and data collection were conducted on three geographically separate institutions of higher learning including Mississippi State University (MSU), St. Cloud State University (SCSU), and Winona State University (WSU). The results described herein are based on data from 481 surveys collected from users, 30 surveys collected from IT professionals, and seven personal interviews of IT professionals.

#### **Overview**

This work draws together two previously unrelated research streams. In light of recent increased attention focused on information security, Innovation Diffusion Theory and security concerns constructs were merged to form a new instrument. A survey was conducted on two separate campuses. 481 usable surveys were collected and analyzed.

Factor analysis revealed favorable factor loadings in the new instrument. However, logistic regression models did not predict wireless use any better than a naïve model which indicated that everyone was a wireless user. Perhaps this is because such a high percentage (89.4%) of respondents indicated their willingness to use wireless.

The absence of significance in the initial model led to construction of six additional logistic regression models. These models used various combinations of the categorical dependent variable and the full data set as well as segregated Mississippi State University (MSU), and Winona State University (WSU) data sets. Further analysis was then conducted with the second dependent variable. This analysis led to the discovery that the constructs of Susceptibility and Severity of Threat, Improvement Potential, and Visibility were significant predictors in the final model.

Case studies were conducted in an effort to gain a deep knowledge of IT professionals' concerns, attitudes, and best practices toward wireless security. A pilot case study was conducted on the campus of Mississippi State University. Cognizant of the experience gained in the pilot case study, additional case studies were conducted on the campuses of St. Cloud State University and Winona State University. Seven IT professionals were personally interviewed regarding their perceptions and attitudes toward wireless security. In an effort to compare IT professional and end user opinions, 30 IT professionals from MSU, SCSU, and WSU completed the survey. Findings indicate that security professionals are very optimistic on the future of wireless computing. However, that optimism is tempered by a realization that there are a myriad of potential threats that might exploit weakness in wireless security.

The results from both the survey and case study were compared in an effort to determine differences and similarities between users' perspectives and managers' perspectives regarding wireless network security. Many IT professionals and users use both wired and wireless networks. However, most IT professionals (76.19%) reported that, all factors considered, they prefer to use wired networks as opposed to wireless networks; whereas, substantially fewer (44.86%) of the student respondents reported that they preferred wired over wireless networks. Overall, results suggest that IT professionals are more concerned about security than are users. It is possible however, that IT professionals may be partial to wired connections as they typically have offices whereas, students typically do not have offices.

In many cases awareness is the first step to providing security (GAO, 1998; Goodhue et al., 1989; Im & Baskerville, 2005; Rhee et al., 2005; Siponen, 2000; Straub et al., 1998). D. Printy indicated that the MnSCU security audit raised awareness to many previously unheard of security concerns. In some cases IT professionals are more conservative in their estimation of preparedness. For example, he graded the wireless security of his network at a nine on a ten point scale but prior to the audit he would have put it at a seven (personal communication, September 13, 2005). However many organizations aren't concerned enough about security until it is too late. S. Kristiansen remarked that many higher level managers have an attitude that security and recovery are a waste of time until there is a breach, but at that point it is too late (personal communication, September 21, 2005). A challenge remains to make administrators and users aware of the full effect of security threats to wireless technologies.

### **A Keen Eye on the Future**

In an effort to provide effective and efficient wireless security, network managers will need to maintain vigilance in staying abreast of the ever changing security milieu.

D. Printy commented that there are new threats that are introduced into the computing environment every week (personal communication, September 13, 2005). Accordingly, security experts need to maintain a keen sense of awareness of the computing environment and stay abreast of not only new threats that emerge in existing categories, but also new categories of threats as they develop. Wireless security adds another level of complexity to efforts to develop a holistic approach to security.

Today's most common wireless encryption protocol, Wired Equivalent Privacy (WEP) is definitely breakable. As long as electromagnetic radiation transverses the personal air space of several potential users, Wi-Fi will be inherently more vulnerable than wired networks (Berghel & Uecker, 2005). In response to this weakness, an emphasis must be placed on maintaining an advantage over computer criminals in regard to wireless encryption and its level of breakability. To be effective, a given security mechanism, such as stronger encryption, needs to be easily implemented by users. Unfortunately, even the best security mechanism is not effective unless it is deployed. At a more pragmatic level, Microsoft has recently announced Wi-Fi Protected Access version 2 (WPA2). WPA2 is touted as more secure than WEP and easily deployed in the Windows XP operating system (Bowman, 2005).



Even with the best prognosticative efforts, it is difficult to determine what the legal system holds for behavior with wireless technologies. As with many other technology related areas, laws and regulations for wireless technologies seem to be lag rapid advances of the technology. Several legal issues remain unresolved with regard to wireless. For example, it remains to be seen if it is a crime to use another's signal without their permission or if network owners are vicariously liable for traffic sent over a network. The recent arrest of a Florida man on charges of unauthorized wireless use will possibly set a precedent for future cases (McCullagh, 2005). Recently, lawmakers in a New York suburb proposed a law that would make it illegal for a business or home office to operate unsecured wireless access points (Broache, 2005). Given these and other potential legal problems, it then becomes critical for those who deploy wireless networks to stay abreast of legal developments effecting the wireless environment.

“In order to maximize benefits from IT investments, organizations must understand and manage their implementation processes” (Cooper et al., 1990). A primary objective of this dissertation is to provide a more precise model to explain critical factors in diffusion of WLANs and to explain how security concerns are balanced with competing factors such as ease of use. Lack of knowledge and technical know how can lead to barriers to diffusion of innovations (Attewell, 1992). Therefore, it is critical to provide adequate training methods on the use of wireless technologies. This research assists in identifying the characteristics of innovators. This knowledge allows for decision makers to better address user training needs.

## Recommendations

At some point an innovation, such as wireless networking, may provide a source of differentiation or possibly even a source of competitive advantage. Organizations that are late implementing new technologies run the risk of falling behind, while conversely, operating on the bleeding edge of technology is not without its own risks (Fichman, 2000). However, the differentiation and competitive advantage that innovations may initially provide diminish as more and more competitors adopt the innovation. For example, where we once saw wireless capabilities emerge in established cyber cafes, now they are becoming commonplace in food and beverage establishments including some fast food restaurants such as McDonalds. It might be logical to conclude in the university setting that wireless networks are rapidly becoming a standard. If this is true, universities and other organizations that offer wireless access such as service stations, communities, coffee shops, and hotels need to place more emphasis on wireless security.

A rogue access point is a functional but unauthorized access point installed in a network. Considering the relative low cost of access points, the ease at which they can be installed, and their small size, the threat of rogue access points can indeed be formidable. Rogue access points can be problematic in that they can allow intruders unauthorized access to the entire network (Sharma, 2004). Because rogue access points can be a large source of concern, network managers need to be keenly aware of the possibility of rogue access points on their networks and take corrective action when they are identified. This is particularly true when business operations are conducted on the network and less so if the wireless network is for customer convenience such as was presented in Schmidt et al.

2004. With the enactment of Sarbanes-Oxley, corporate executives must personally sign to guarantee the quality and integrity of the information within an information system (Volonino, Gessner, & Kermis, 2004). This act has increased the potential for litigation regarding information systems. If a computer criminal gains malicious access to an organization's network via a rouge wireless access point, executives run the risk of being held personally liable for damages. Future protection mechanisms will need to rapidly determine the existence of such points and mitigate their potential for being exploited.

### **Limitations**

When done properly, research will advance knowledge for the benefit of the scientific community (Dennis et al., 2001). Indeed, when research adheres to scientific principles the outcome is likely to benefit several stakeholders including the academic and practitioner communities. However, it is important to consider that all research is inherently flawed in some form or another (Dennis et al., 2001). Realizing this limitation, it is prudent to evaluate research on the dimensions of generalizability, realism, and precision (McGrath, 1981).

An effective approach to address the flaws in each method is to use a combination of methods to produce results that are generalizable, realistic, and precise. Simultaneous use of multiple methodologies will generate fruitful research for IS scholars (Nunamaker Jr. et al., 1990 / 1991). To that end, this research employed the case study and survey methods to gain a greater level of understanding of perceptions of wireless networks and their corresponding security concerns. In order to generalize the findings to the

population as a whole, it may still be necessary to further test the research hypotheses based on data from a truly random sample of the population.

When conducting survey research, it is wise to consider the situation and circumstances regarding the data collection method. The survey instrument included five pages on which respondents answered questions and an additional page which was used as a consent form. Respondents were asked to provide answers to 17 demographic questions, 31 questions that were considered independent variables, two questions that were considered dependent variables, and six open ended questions. Based on the length of the survey, it could be argued that fatigue may have been a factor for some respondents. Additionally, for many respondents there was little or no vested interest in providing the best, most well constructed answers to the questions. Taken together, these factors regarding the data collection may be construed as a potential limitation of this, or any, survey research.

Another possible criticism of this research involves the tradeoff between an all inclusive model and a parsimonious model with which respondents will not experience fatigue while completing the survey instrument. There are many factors that may exert an impact on decision behavior under risk. Several of those items include risk preferences, inertia, outcome history, problem framing, top management team homogeneity, social influence, problem domain familiarity, and organizational control systems (Sitkin et al., 1992).

While the interviews for the case study portion utilized IT professionals, the data to test the research hypotheses were obtained from students. Pundits may criticize

research conducted with a student sample. However, as Sitkin and Weingart (1995) suggest, the use of students as research subjects is valid as long as researchers are cognizant of the population to which they can generalize. Further, as D. Straub indicated, students are not always useful research subjects, but they are very useful in research that attempts to uncover how people think (personal communication, April 15, 2005). It could easily be argued that students are the logical choice involving research of wireless adoption and security as this group is more likely than the population at large to understand and use wireless technologies. The reader is then left to determine whether or not students are reasonable subjects for the research at hand.

Cronbach's alpha is the most widely used measure of consistency within a scale (Hair Jr. et al., 1998). A Cronbach's alpha of .70 or higher is typically needed to consider a scale as valid, while it has been suggested that in some cases, a Cronbach's alpha of .60 is considered adequate (Garson, 2005; Hair Jr. et al., 1998). Four of the seven scales used herein had Cronbach's alphas of .85 or higher. However, the constructs of Voluntariness, Visibility, and Trialability had Cronbach's alphas of .688, .632, and .620 respectively. Given these relatively low numbers, it is possible that there are measurement confounds present in this research.

In one study, there was evidence that measurement confounding did not necessarily account for the association between two variables (Lemery, Essex, & Smider, 2002). Nevertheless, there may have been confounding between items in the instrument. Other issues that might have affected the research are that some of the items loaded differently than anticipated. For instance, the three items from the original constructs of

Perceived Severity of Threat and the three items from Perceived Susceptibility to Threat all loaded together.

Additionally, there are many factors that may have additional impact on student perceptions, including a student's previous experience, propensity to embrace new technologies, and perhaps whether a student currently has a computer with wireless capabilities. These constructs were reserved for future research in favor of developing a questionnaire that will not evoke negative reactions.

### **Direction for Future Research**

Innovation Diffusion Theory is adaptable for specific situations. Recently, Chandra & Calderon (2005) proposed that additional issues such as privacy and trust play a role in the decision to adopt biometrics thus effecting traditional adoption models. In a similar fashion, a security construct was added to the well established PCI Model. The research model can be refined in future research. One such refinement could be to include an additional construct to measure the sensitivity of the task. A construct termed "Sensitivity of Task" would take into consideration the users' perception of what they may have to lose if a security breach were to occur. The addition of this construct might allow the model to be more flexible in regard to user propensity to adopt. For instance, a user may choose to adopt a given technology for certain applications and not others. For the topic at hand, perhaps users will use a wireless connection to surf the web but will hesitate to use wireless if passwords are involved (e.g. checking email or conducting online banking).

While the factor analysis procedure was successful in legitimizing the synthesized instrument; logistic regression procedures failed to identify significant relationships between the dependent variable and the factors of Improvement Potential, Usage, Susceptibility and Severity of Threat, Image, Voluntariness, Visibility, and Trialability. Given that 89.4% of respondents indicating their willingness to use wireless in a security sensitive paradigm, the logistic regression model is equivalent to a naïve model which simply predicts everyone will use wireless.

Fortunately, multiple regression techniques using a scaled dependent variable produced enough statistical evidence to conclude that the constructs of Susceptibility and Severity of Threat, Improvement Potential, and Visibility were significant predictors of users' level of security concern for using wireless in sensitive transactions. Further research should be conducted with technology that has a more even split between users and non-users. With a more even split between users and non-users it is possible that many of the aforementioned constructs will be significant in predicting diffusion of wireless network technologies.

A social system can be thought of as a “collectivity of units which are functionally differentiated and engaged in joint problem solving with respect to a common goal” (Rogers et al., 1971, p. 28). Given the preceding definition, it is quite logical to view a typical university as a social system. Given the nature of the university social system, the adoption of WLANs on college campuses may experience a somewhat compressed S-curve within the categories of innovators, early adopters, early majority, and laggards. Although beyond the nature and scope of this dissertation, future research

should address the rate at which wireless networks have diffused through various universities. Network administrators commented on the rapid pace at which wireless diffused on their campuses. If researchers could uncover precisely the reasons why, then better pre-deployment planning could be employed by both academicians and practitioners for subsequent technology deployments.

A logical assumption is that persons more aware of threats and security inadequacy would be more likely to have the perception that security was unsatisfactory. “Thus all other things being equal, we would expect that the greater awareness of potential abuse would lead to more concern about security, and perceptions that the environment was more unsatisfactory” (Goodhue et al., 1989, p. 120). The question of whether persons with technical backgrounds perceive the level of threat to be more important then comes to mind. A future study that focuses on IT professionals could be undertaken to address this issue.

“All things being equal, we would expect persons in industries with a high degree of security danger to be more concerned about security” (Goodhue et al., 1989, p. 120); accordingly, one might expect that persons involved in such endeavors as banking and finance may have a greater concern for security threats than would students in a university setting. A survey involving employees in industries with high security danger such as banking could be undertaken to determine if such professionals are more concerned about security than college students.

After the interviews with IT professionals, it became evident that the use of the initial, if not any, taxonomy of threats was problematic. Based on the seemingly clear



distinction between malicious and act of God categories of threat. This characteristic might fit better on the first level of the taxonomy rather than the third level as in the original taxonomy. It may very well be that interviewees would have an easier task of characterizing threats as malicious or an act of God to start the process. After the question of intent was addressed, interviewees would then be asked to further categorize the threats based on location in the case of malicious threats or in the case of act of God, further characterize threats based on their source. Figure 5.1 presents the modified taxonomy of threats. This taxonomy could be used in future interviews with IT professionals.

Malicious		Act of God		
Internal	External	Natural Disaster	Equipment Failure	Human Error

Figure 5.1: Modified Taxonomy of Threats

Further research is needed in regard to Innovation Diffusion Theory (IDT) and security risk factors for wireless networks. While the results of this study provide clear evidence for the impact of security risk, they raise several questions in terms of confirming or refuting IDT in this context. Specifically, Perceived Susceptibility and Severity to Threat were found to be significant predictors while two of the six factors

from IDT (Improvement Potential and Visibility) were found to be significant predictors. Speculation may lead one to believe that a different frame of reference for the dependent variable may have produced more conclusive results. However, even the best prognosticative efforts will not provide the answer. To address these issues, future research with the same independent variables and a modified dependent variable may provide the answer.

### **Contributions**

The results provide additional insight to academicians and practitioners alike. Previous studies have developed instruments to address Innovation Diffusion, Perceived Characteristics of Innovating, and Perceived Susceptibility and Severity to Threat. This study attempted to synthesize constructs from the aforementioned studies. Factor analysis revealed seven factors (Improvement Potential, Usage, Susceptibility and Severity of Threat, Image, Voluntariness, Visibility, and Trialability) that can be measured by 31 individual items. The resulting instrument is intended to provide academicians a mechanism to measure diffusion at the individual level in light of security factors. Practitioners can use the results in estimating how certain technologies will be received and adopted in the marketplace.

Existing taxonomies of threat to information systems are widely accepted. However, due to the paradigm of new threat emergence, such taxonomies are inadequate for today's security milieu. Another issue that makes many threat taxonomies insufficient is the blended threat. Blended threats involve combining worms, viruses,

Trojans, and other mechanisms to exploit vulnerabilities. Blended threats are particularly troublesome with email (Forte, 2004). In the past it was possible to analyze threats and efficiently place them in one of several categories. However, today that appears to be increasingly difficult. As a result the taxonomy as depicted in figure 5.1 may provide a more effective manner to characterize risk.

There appears to be a push for ubiquitous wireless access in today's connectivity milieu. Wireless access is assumed by its users to be like a utility. This is particularly evident on college campuses, especially on campuses with laptop requirements such as WSU. The vice president of technology at WSU typified that sense when he commented that the wireless network on his campus is like water or electricity because, if it is not up and running 24 hours a day seven days a week, users will demand that it be fixed immediately. A network technician at WSU observed how fast users moved from a point of being impressed by wireless access to feeling upset if they experience dead spots on campus. He further observed that wireless was the fastest technology adoption by end users that he has ever seen and once it was in place it was like it had always been there.

Perceptions of performance are frequently loosely tethered to actual performance (Ehrlinger & Dunning, 2003). Almost all IT professionals rated their level of preparedness to deal with threats posed to wireless security as higher than other similar organizations. In fact, five out of the six IT professionals who provided answers to these questions (seven IT professionals were interviewed, however, one person who was interviewed early in the interview process was no longer employed by the institution when the final series of questions were posed) indicated that they were better prepared in

relation to their counterparts. The only IT professional who didn't rate his level of preparedness higher than others' level of preparedness rated his organization at an eight and placed the others' level in a range from seven to nine.

On a ten point scale, IT professionals perceived their level of preparedness at an average of 7.8 while perceiving their counterparts at an average of 5.4. The perception that one is better prepared than his or her neighbors leads to a question of overconfidence. If IT professionals are overconfident, there is a danger. Although none of the professionals seemed to be overconfident or arrogant about their security plan, the fact remains that everyone cannot be above average. Unfortunately, it might be that people have an "average" level of protection but think their level of protection is above average. These people are therefore potentially at risk of falling into complacency and thus their networks are more vulnerable to attack. Given a tendency to self-overrate, it would then be wise to seek an unbiased opinion from an outside consultant who can objectively evaluate a firm's security measures. This falls short of a call for complete outsourcing of security management, but recognizes the importance of independent counsel.

In 1995, Eric Schmidt, Chief Technology Officer at Sun Microsystems reported that almost all the customers he spoke with did not have a detailed security plan (Wingfield, 1995). Perhaps in part due to recent high profile computer security events, more organizations are taking computer security more seriously. In fact over 87% of surveyed organizations conducted security audits in 2004 up from 82% in 2003 (Computer Security Institute, 2005). Unfortunately, computer security is a moving target and poses a constant battle to those charged with providing it.

Based on the findings uncovered during the interviews with the seven managers, a strong opinion emerged that IT can never be perfectly secured in the university environment. The security milieu is such that one network technician declared that the only way to be 100% secure is to turn the device off and even then he wouldn't make any guarantees. Given the nature of the business world where billions of dollars trade hands electronically every day, it is even less likely that it is possible to achieve total security. Because system failure is inevitable, systems must be designed with a mechanism to provide notification when a failure does occur (Campbell, 2006).

Once an existing security threat is addressed by security professionals, computer criminals are eager to evolve and attack other vulnerabilities in the system (Campbell, 2006). The unfortunate consequence is that information system security professionals need to protect their systems from all possible vulnerabilities while computer criminals simply need only one vulnerability to exploit. Because of this asymmetrical nature of information security, security professionals need to maintain a keen awareness of both new and existing threats.

### **Conclusions**

The multimethodological approach utilized in this dissertation, used both the survey and case study techniques. There are findings unique to the survey portion, unique to the case study portion, and findings which only present themselves when results from the two above techniques are synthesized. Therefore, the conclusions are summarized with survey, case, and survey synthesis in mind.

To address the study goal of extending Moore and Benbasat's (1991) PCI model to include security constructs 481 useable surveys were analyzed in an effort to add the constructs of perceived susceptibility to threat and perceived severity to threat. Two previously validated instruments were synthesized and revised to create a new instrument to test this model. The factor analysis procedure was successful in condensing 31 items into seven factors.

Logistic regression analysis was utilized with the seven factors identified during factor analysis. The dependent variable of wireless use was regressed on the aforementioned seven factors. Unfortunately, the resulting model simply predicts that everyone is a user of wireless. In doing so, the model achieves 89.4% accuracy. This is likely due to the fact that of 481 respondents only 51 indicated that they would not use wireless to check their account in the fictitious scenario. Future research should be conducted in such a manner that allows a more equal split between users and non-users. In doing so, there may prove to be more predictive power in the resulting model.

Because the seven constructs were not significant with this particular dependent variable, it was not appropriate to determine if there were interaction effects between the threat and other constructs. Future research will address the interaction between the security construct and the other six constructs.

Fortunately, further data analysis and model construction with a second dependent variable yielded significant results. This analysis led to the discovery that the constructs of Susceptibility and Severity of Threat, Improvement Potential, and Visibility were

significant predictors in the final model. These findings should provide a starting point for future research in the area.

The case study method was utilized to extend the knowledge base regarding security considerations of wireless network implementations in a university environment. After a pilot case study, two additional case studies were conducted in an effort to achieve this goal. In total, seven IT professionals were personally interviewed regarding their perceptions of wireless data networks. Additionally, four of those seven IT professionals as well as 26 IT professionals completed surveys concerning wireless security.

Among the interesting findings is the fact that managers generally consider their wireless networks to be relatively more secure than other wireless networks in similar organizations. It is possible that this may lead to a sense of overconfidence on the part of network managers and further lead to a sense of complacency and increased vulnerability. To negate the effects of such a possibility, it is suggested that practitioners seek a neutral observer's assessment in an effort to decrease the vulnerability to threats in their environment. Whether this assessment is accomplished by outsiders from experienced security firms or insiders with an in-depth knowledge of the campus and its network is another management issue, but it must be done when the wireless network begins and then on a periodic basis as both technologies and attack methods change. Even though network managers are keenly aware that there is a dearth of perfect security in regard to information systems, the effort to approach perfection should not be abandoned.

Confounding the problems posed by wireless security is the nature of demand for wireless services. Likely due to the convenience and portability offered by wireless access, there appears to be a push for ubiquitous access to wireless. The availability of wireless access is assumed by end-users. Users have made a rapid progression from a point of being impressed by wireless access to a point of becoming upset when there are difficulties obtaining access for a particular time and place. Organizations should therefore provide mechanisms to quickly and easily report difficulties with wireless access and once problems are reported, they should be addressed immediately. One way in which this could be accomplished is by implementing a system whereby wireless access points continuously communicate their operation status to other access points within range. In that way, network managers could easily be notified if there were technical difficulties with one or more access points.

The results from both the survey and case study were compared and synthesized in an effort to determine differences and similarities between users' perspectives and managers' perspectives regarding wireless network security. IT professionals appear to absorb the brunt of security threats in the environment. Because IT professionals take adequate precautions, they can provide an environment in which users feel relatively secure using wireless technologies.

IT professionals were more likely to prefer a wired network whereas end-users were more likely to prefer a wireless network. Qualitative data analysis suggests that IT professionals prefer wired because of security concerns with wireless. Students on the other hand appear to prefer wireless networks based on the convenience afforded by



wireless. Although the dual nature of convenience and security has long existed, it must be examined in light of these differences in user groups' perceptions. In cases where facts overshadow inaccurate perceptions, these discrepancies must be brought to the surface and addressed.

Growth of wireless networks and the increasing demand from consumers for ubiquitous information access will likely continue unabated for the foreseeable future. As this trend continues, a new computing paradigm will likely evolve. Already, services for high speed wireless access are beginning to take hold and entire communities are adopting plans to develop mesh networks allowing wireless access over large geographic areas. If users are to safely and securely operate in the new wireless milieu, much work is needed in effort to develop both technical and procedural controls to ensure the confidentiality, availability, integrity, and accountability of data and information within that milieu.

## BIBLIOGRAPHY

- Aczel, A. D. (1999). *Complete Business Statistics, 4th Edition*. Boston, MA: Irwin McGraw-Hill.
- Agarwal, R., & Prasad, J. (1997). The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies. *Decision Sciences*, 28(3), 557-582.
- Agarwal, R., & Prasad, J. (2000). A Field Study of the Adoption of Software Process Innovations by Information Systems Professionals. *IEEE Transactions on Engineering Management*, 47(3), 295-308.
- Albright, S. C., Winston, W. L., & Zappe, C. (2002). *Managerial Statistics*. Pacific Grove, CA: Wadsworth / Duxbury.
- Antonio, A. L. (2004). The Influence of Friendship Groups on Intellectual Self-Confidence and Educational Aspirations in College. *Journal of Higher Education*, 75(4), 446-471.
- Applegate, L. M., Austin, R. D., & McFarlan, F. W. (2003). *Corporate Information Strategy and Management: The Challenges of Managing in a Network Economy*. Boston, MA: McGraw-Hill.
- Ash, J. S. (1997). *Factors Affecting the Diffusion of the Computer-Based Patient Record*. Paper presented at the Journal of the American Medical Informatics Association Supplement.
- Attaway, M. (2003, June). Protecting Against Wireless Threats. *Internal Auditor*, 60, 26-29.
- Attewell, P. (1992). Technology Diffusion and Organizational Learning: The Case of Business Computing. *Organization Science*, 3(3), 1-18.
- Austin, R. D., & Darby, C. A. R. (2003). The Myth of Secure Computing. *Harvard Business Review*, 81(6), 120-126.

- Ball, L., & Harris, R. (1982). SMIS Members: A Membership Analysis. *MIS Quarterly*, 6(1), 19-38.
- Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3), 368-386.
- Benbasat, I., Goldstein, D. K., & Mead, M. (1988). Issues and Opinions. *MIS Quarterly*, 12(4), 522.
- Berghel, H., & Uecker, J. (2005). WiFi Attack Vectors. *Communications of the ACM*, 48(8), 21-28.
- Bishop, M. (2003). *Computer Security Art and Science*. Boston, MA: Addison-Wesley.
- Blackwell, G. (2002). Assessing Total Cost of Ownership. Retrieved May 2, 2005, from <http://www.wi-fiplanet.com/tutorials/article.php/953691>
- Bleicher, P. (2000). Wireless in Seattle--and Everywhere Else. *Applied Clinical Trials*, 9(6), 36-37.
- Borisov, N., Goldberg, I., & Wagner, D. (2001). *Intercepting Mobile Communications: The Insecurity of 802.11*. Paper presented at the International Conference on Mobile Computing and Networking, Berkeley, CA.
- Bowman, B. (2005). Implement WPA2-Personal wireless security on a Windows XP SP2-based computer. from [http://www.microsoft.com/windowsxp/using/security/expert/bowman\\_wirelesssecurity.msp](http://www.microsoft.com/windowsxp/using/security/expert/bowman_wirelesssecurity.msp)
- Brancheau, J. C., & Wetherbe, J. C. (1990). The Adoption of Spreadsheet Software: Testing Innovation Diffusion Theory in the Context of End-User Computing. *Information Systems Research*, 1(2), 115-143.
- Broache, A. (2005). Unsecured Wi-Fi Would be Outlawed by N.Y. County [Electronic Version]. *ZDNet Wired & Wireless*. Retrieved November 5, 2005 from [http://news.zdnet.com/2100-1035\\_22-5934194.html](http://news.zdnet.com/2100-1035_22-5934194.html).
- Campbell, S. (2006). How to Think About Security Failures. *Communications of the ACM*, 49(1), 37-39.

- Carlson, J. R., & Zmud, R. W. (1999). Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions. *Academy of Management Journal*, 42(2), 153-170.
- Carlson, R. O. (1965). *Adoption of Educational Innovations*. Eugene, OR: Center for the Advanced Study of Educational Administration.
- Carnevale, D. (2004, October, 29). Fewer Colleges Cut Information-Technology Budgets This Year, Survey Finds. *Chronicle of Higher Education*, 51.
- Chandra, A., & Calderon, T. (2005). Challenges and Constraints to the Diffusion of Biometrics in Information Systems. *Communications of the ACM*, 48(12), 101 - 106.
- Chen, L., & Nath, R. (2003). *Implementing and Managing Wireless LAN: An Empirical Study*. Paper presented at the Ninth Americas Conference on Information Systems (AMCIS), Tampa, FL.
- Chordas, L. (2004, September). Chubb Underwriter: Businesses Need To Be More Serious About IT Risks. *Best's Review*, 105, 96.
- Cisco Systems Inc. (2005). Wireless Standards. Retrieved March 3, 2005, from <http://www.linksys.com/edu/wirelessstandards.asp>
- Coleman, J., Katz, E., & Menzel, H. (1966). *Medical Diffusion: An Innovation Study*. Indianapolis, IN: Bobbs-Merrill.
- Computer Security Institute. (2003). 2003 CSI/FBI Computer Crime and Security Survey. Retrieved July 26, 2003, from [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2003.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf)
- Computer Security Institute. (2004). 2004 CSI/FBI Computer Crime and Security Survey. Retrieved February 5, 2005, from [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2004.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf)
- Computer Security Institute. (2005). 2005 CSI/FBI Computer Crime and Security Survey. Retrieved January 13, 2006, from <http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf>
- Congress Triples Cyber Security Funding. (2003). *Information Management Journal*, 37(1), 14.

- Cooper, R. B., & Zmud, R. W. (1990). Information Technology Implementation Research: A Technological Diffusion Approach. *Management Science*, 36(2), 123-139.
- Covert, E., & Nielsen, F. (2005). Measuring Risk Using Existing Frameworks. *Information Systems Security*, 14(1), 21-25.
- Cragg, P. B., & King, M. (1993). Small-Firm Computing: Motivators and Inhibitors. *MIS Quarterly*, 17(1), 47-60.
- Daniel, E. M., & Grimshaw, D. J. (2002). An Exploratory Comparison of Electronic Commerce Adoption in Large and Small Enterprises. *Journal of Information Technology*, 17(3), 133-147.
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 318-340.
- Dean, T. (2003). *Guide to Telecommunications Technology*. Boston, Massachusetts: Thomson Course Technology.
- Dell Inc. (2005). *A Complete Technology Solution for your Campus*.
- Dennis, A. R., & Valacich, J. S. (2001). Conducting Research in Information Systems. *Communications of the Association for Information Systems*, 7(5), 1-40.
- DeSanctis, G., & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science: A Journal of the Institute of Management Sciences*, 5(2), 121-147.
- Deval, M., Khosravi, H., Muralidhar, R., Ahmed, S., Bakshi, S., & Yavatkar, R. (2003). Distributed Control Plane Architecture for Network Elements. *Intel Technology Journal*, 7(4), 51-63.
- Dickson, G. W., Leitheiser, R. L., Wetherbe, J. C., & Nechis, M. (1984). Key Information Systems Issues for the 1980's. *MIS Quarterly*, 8(3), 135-148.
- Drew, S. (2005). Reducing Enterprise Risk with Effective Threat Management. *Information Systems Security*, 13(6), 37-42.
- Dubé, L., & Paré, G. (2003). Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly*, 27(4), 597-635.
- Dudman, J. (2004, November, 9). Manning the Breaches. *Computer Weekly*, 52-54.

- Durrington, V. A., Repman, J., & Valente, T. W. (2000). Using Social Network Analysis to Examine the Time of Adoption of Computer-Related Services among University Faculty. *Journal of Research on Computing in Education*, 33(1), 16-27.
- Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1), 67-87.
- Ehrlinger, J., & Dunning, D. (2003). How Chronic Self-Views Influence (and Potentially Mislead) Estimates of Performance. *Journal of Personality & Social Psychology*, 84(1), 5-16.
- Fichman, R. G. (1992, December). *Information Technology Diffusion: A Review of Empirical Research*. Paper presented at the Proceedings of the Thirteenth International Conference on Information Systems (ICIS), Dallas, TX.
- Fichman, R. G. (2000). The Diffusion and Assimilation of Information Technology Innovations. In R. Zmud (Ed.), *Framing the Domains of IT Management: Projecting the Future Through the Past*. Cincinnati, OH: Pinnaflex Publishing.
- Fichman, R. G., & Kemerer, C. F. (1999). The Illusory Diffusion of Innovation: An Examination of Assimilation Gaps. *Information Systems Research*, 10(3), 255-275.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Boston, MA: Addison-Wesley.
- Forte, D. (2004). MyDoom & Co. is There Really a Problem? *Network Security*, 2004(3), 14.
- Furnell, S. M., Papadaki, M., Magklaras, G., & Alayed, A. (2001). Security Vulnerabilities and System Intrusions: The Need for Automated Response Frameworks. In H. P. Eloff, L. Labuschage, R. V. Solms & G. Dhillon (Eds.), *Advances in Information Security Management & Small Systems Security*. Dordrecht, Netherlands: Kluwer Academic Publishers.
- GAO. (1998). *Information Security Management*. Washington, DC: General Accounting Office.
- Garson, G. D. (2005). Factor Analysis [Electronic Version]. Retrieved November 11, 2005 from <http://www2.chass.ncsu.edu/garson/pa765/garson.htm>.

- Gerbing, D. W., & Anderson, J. C. (1988). An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment. *Journal of Marketing Research*, 25(2), 186-192.
- Goodhue, D. L., & Straub, D. W. (1989). *Security Concerns of System Users: A Proposed Study of User Perceptions of the Adequacy of Security Measures*. Paper presented at the Proceedings of the Twenty-Second Annual Hawaii International Conference on System Science (HICSS), Kailua-Kona, HI.
- Grapentine, T. (1995). Dimensions of an Attribute. *Marketing Research*, 7(3), 18-27.
- Green, G. C., & Hevner, A. R. (2000). The Successful Diffusion of Innovations: Guidance for Software Development Organizations. *IEEE Software*, 17(6), 96-103.
- Green, K. C. (2003, October). The 2003 National Survey of Information Technology in US Higher Education. from <http://www.campuscomputing.net/summaries/2003/>
- Green, K. C. (2005). The 2005 National Survey of Information Technology in US Higher Education. from <http://campuscomputing.net/>
- Hair Jr., J. H., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis* (5 ed.). Upper Saddle River, New Jersey: Prentice Hall.
- Hardgrave, B. C., Davis, F. D., & Riemenschneider, C. K. (2003). Investigating Determinants of Software Developers' Intentions to Follow Methodologies. *Journal of Management Information Systems*, 20(1), 123-152.
- Hartog, C., & Herbert, M. (1986). 1985 Opinion Survey of MIS Managers: Key Issues. *MIS Quarterly*, 10(4), 350-361.
- Hayes, F. (2002, June 24). Security: Today's Y2K. *Computerworld*, 36, 1-2.
- Hoffer, J. A., & Alexander, M. B. (1992). The Diffusion of Database Machines. *Data Base* 23, 13-19.
- Hoffer, J. A., & Straub Jr., D. W. (1989). The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review*, 30(4), 35-44.
- Hollis, E. (2004, December). WLAN Switching: Managing Wireless Access Points. *Certification Magazine*, 6, 42.

- Im, G. P., & Baskerville, R. L. (2005). A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. *The DATA BASE for Advances in Information Systems*, 36(4), 68-79.
- Kaefer, F., & Bendoly, E. (2004). Measuring the Impact of Organizational Constraints on the Success of Business-to-Business E-Commerce Efforts: A Transactional Focus. *Information & Management*, 41(5), 529-541.
- Kahai, P. S., & Kahai, S. K. (2004). Deployment Issues and Security Concerns With Wireless Local Area Networks: The Deployment Experience at a University. *Journal of Applied Business Research*, 20(4), 11-24.
- Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly*, 23(3), 183-213.
- Keen, P. G. W. (1980). *MIS Research: Reference Disciplines and a Cumulative Tradition*. Paper presented at the International Conference on Information Systems (ICIS).
- Keen, P. G. W., & Woodman, L. A. (1984). What to do with all those Micros. *Harvard Business Review*, 62(5), 142-149.
- Keil, M., Cule, P. E., Lyytinen, K., & Schmidt, R. C. (1998). A Framework for Identifying Software Project Risks. *Communications of the ACM*, 41(11), 76-83.
- Kendall, K. E., & Kendall, J. E. (2002). *Systems Analysis and Design* (5 ed.). Upper Saddle River, New Jersey: Prentice Hall.
- King, R. (2004). Techsoup. Retrieved March 24, 2005, from [http://www.techsoup.org/community/qod\\_answer.cfm?qotdid=7&topicid=3](http://www.techsoup.org/community/qod_answer.cfm?qotdid=7&topicid=3)
- Kraut, R. E., Rice, R. E., Cool, C., & Fish, R. S. (1998). Varieties of Social Influence: The Role of Utility and Norms in the Success of a New Communication Medium. *Organization Science: A Journal of the Institute of Management Sciences*, 9(4), 437-453.
- Lally, L. (2005). Information Technology as a Target and Shield in the Post 9/11 Environment. *Information Resources Management Journal*, 18(1), 14-28.
- Lauer, J. M., & Asher, J. W. (1988). *Composition Research: Empirical Designs*: Oxford University Press, USA.



- Laver, M. (2003). Awareness of Wireless Fidelity Taking Off. Retrieved February 19, 2004, from <http://www.ipsos-na.com/news/pressrelease.cfm?id=1750>
- Lee, A. S. (1989). A Scientific Methodology for MIS Case Studies. *MIS Quarterly*, 13(1), 32-50.
- Lee, A. S., & Liebenau, J. (1997). Information Systems and Qualitative Research. In A. S. Lee, J. Liebenau & J. deGross (Eds.), *Information Systems and Qualitative Research*. London: Chapman & Hall.
- Lee, A. S., & Weber, R. (2004). *A Framework for Linking Theory, Practice, and Curriculum: The Instance of Offshore Outsourcing in the Discipline of Information Systems*. Paper presented at the International Conference on Information Systems (ICIS), Washington, D.C.
- Lee, J. (2004). Discriminant Analysis of Technology Adoption Behavior: A Case of Internet Technologies in Small Businesses. *Journal of Computer Information Systems*, 44(4), 57-66.
- Lemery, K. S., Essex, M. J., & Smider, N. A. (2002). Revealing the Relation between Temperament and Behavior Problem Symptoms by Eliminating Measurement Confounding: Expert Ratings and Factor Analyses. *Child Development*, 73(3), 867-882.
- Lewis, W., Agarwal, R., & Sambamurthy, V. (2003). Sources of Influence on Beliefs about Information Technology Use: An Empirical Study of Knowledge Workers. *MIS Quarterly*, 27(4), 657-678.
- Loch, C. H., & Huberman, B. A. (1999). A Punctuated-Equilibrium Model of Technology Diffusion. *Management Science*, 45(2), 160-177.
- Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, 16(2), 173-186.
- Luftman, J., & McLean, E. R. (2004). Key Issues for IT Executives. *MIS Quarterly Executive*, 3(2), 89-104.
- Lytras, M. D. (2005). An Interview with Robert Zmud. from [http://www.sigsemis.org/columns/interviews/zmoud\\_interview](http://www.sigsemis.org/columns/interviews/zmoud_interview)
- Lyytinen, K. (1999). Empirical Research in Information Systems: On the Relevance of Practice in Thinking of IS Research. *MIS Quarterly*, 23(1), 25-27.

- Lyytinen, K., & Robey, D. (1999). Learning Failure in Information Systems Development. *Information Systems Journal*, 9(2), 85-101.
- MacCallum, R. C., & Austin, J. T. (2000). Applications of Structural Equation Modeling in Psychological Research. *Annual Review of Psychology*, 51(1), 201-226.
- Mahajan, V., & Peterson, R. A. (1985). *Models for Innovation Diffusion*. Newbury Park, CA: SAGE Publications.
- Malaga, R. A. (2005). *Information Systems Technology*. Upper Saddle River, NJ: Pearson Prentice Hall.
- Mariko, S. O., Mariko, J. A., & Mariko, B. K. (2003). Adoption of Broadband Internet in Korea: the Role of Experience in Building Attitudes. *Journal of Information Technology*, 18(4), 267-280.
- Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, 10(1), 5-12.
- McCullagh, D. (2005). FAQ: Wi-Fi Mooching and the Law [Electronic Version]. *ZDNet Wired & Wireless*. Retrieved November 5, 2005 from [http://news.zdnet.com/2100-1035\\_22-5778822.html](http://news.zdnet.com/2100-1035_22-5778822.html).
- McGrath, J. E. (1981). Dilemmatics: The Study of Research Choices and Dilemmas. *American Behavioral Scientist*, 25(2), 179-210.
- McKeown, P. (2003). *Information Technology & the Networked Economy* (2 ed.). Boston, MA: Course Technology Thomson Learning.
- Merhout, J. W., & Lee, A. S. (2004). *A Positivist Methodology for Archival Case Studies in Information Systems Research*. Paper presented at the Tenth Americas Conference on Information Systems, New York, New York.
- Microsoft. (2004). Tablet PC on the Go: Scenarios for Powerful Mobile Computing. Retrieved January, 25, 2005, from <http://www.microsoft.com/windowsxp/tabletpc/evaluation/scenarios/corridor.mspx>
- Microsoft. (2005). Wireless Network Security. Retrieved April 29, 2005, from [http://www.microsoft.com/hardware/broadbandnetworking/10\\_concept\\_wireless\\_security.mspx](http://www.microsoft.com/hardware/broadbandnetworking/10_concept_wireless_security.mspx)

- Miller, M. D., Rainer Jr., R. K., & Harper, J. (1997). The Unidimensionality, Validity, and Reliability of Moore and Benbasat's Relative Advantage and Compatibility Scales. *Journal Of Computer Information Systems*, 38(1), 38-46.
- Mingers, J. (2001). Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research*, 12(3), 240-259.
- Minnesota Office of the Legislative Auditor. (2005). Minnesota State Colleges and Universities Wireless Network Security Audit Retrieved October 20, 2005, from <http://www.auditor.leg.state.mn.us/fad/pdf/fad0548.pdf>
- Moore, G. C. (1987). End User Computing and Office Automation: A Diffusion of Innovations Perspective. *Information Management & Computer Security*, 25(3), 214-235.
- Moore, G. C., & Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research*, 2(3), 192-222.
- Myers, M. D. (2001). Qualitative Research in Information Systems. Retrieved April, 27, 2004, from [http://www.cybernurse.org.uk/qualitative\\_and\\_quantitative\\_research.htm](http://www.cybernurse.org.uk/qualitative_and_quantitative_research.htm)
- New Media Consortium. (2005). *The Horizon Report*. Stanford, CA.
- Nobel, C. (2005, January). Companies Find Wi-Fi's Hot Spots. *eWeek*, 22, 1-2.
- NotebookReview.com. (2005). Top 50 Wireless College Campus' in the USA 2005 Results [Electronic Version]. Retrieved October 18, 2005 from <http://www.notebookreview.com/default.asp?newsID=2572>.
- Nunamaker Jr., J. F., Chen, M., & Purdin, T. D. M. (1990 / 1991). Systems Development in Information Systems Research. *Journal of Management Information Systems*, 7(3), 89-106.
- O'Brien, J. (2001). *Introduction to Information Systems Essentials for the Internetworked E-Business Enterprise* (10 ed.). Boston: McGraw-Hill Irwin.
- Oz, E. (2002). *Management Information Systems* (3 ed.). Boston, MA: Course Technology Thomson Learning.

- Pablo, A. L., Sitkin, S. B., & Jemison, D. B. (1996). Acquisition Decision-Making Processes: The Central Role of Risk. *Journal of Management Information Systems*, 22 (5), 723-746.
- Palvia, P., Mao, E., Midha, V., Pinjani, P., & Salam, A. F. (2004). Research Methodologies in MIS: An Update. *Communications of the Association for Information Systems*, 14, 526-542.
- Palvia, P., Mao, E., Salam, A. F., & Soliman, K. S. (2003). Management Information Systems Research: What's There in a Methodology? *Communications of the Association for Information Systems*, 11(11), 289-308.
- Panko, R. R. (2003). *Business Data Networks and Telecommunications* (4 ed.). Upper Saddle River, NJ: Prentice Hall.
- Parthasarathy, M., & Bhattacharjee, A. (1998). Understanding Post-Adoption Behavior in the Context of Online Services. *Information Systems Research*, 9(4), 362-380.
- Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in Computing* (3 ed.). Upper Saddle River, New Jersey: Prentice Hall.
- Phifer, L. (2003). Securing Wireless Access to Mobile Applications. *Business Communications Review*, 33(9), 47-51.
- Plouffe, C. R., Hulland, J. S., & Vandenbosch, M. (2001). Research Report: Richness Versus Parsimony in Modeling Technology Adoption Decisions--Understanding Merchant Adoption of a Smart Card-Based Payment System. *Information Systems Research*, 12(2), 208-222.
- Rhee, H.-S., Ryu, Y., & Kim, C.-T. (2005). *I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security*. Paper presented at the Twenty-Sixth International Conference on Information Systems, Las Vegas, NV.
- Richins, M. L., & Dawson, S. (1992). A Consumer Values Orientation for Materialism and Its Measurement: Scale Development and Validation. *Journal of Consumer Research*, 19(3), 303-316.
- Rogers, E. M. (1962). *Diffusion of Innovations*. New York, New York: The Free Press of Glencoe.
- Rogers, E. M. (1983). *Diffusion of Innovations* (3 ed.). New York, New York: The Free Press.

- Rogers, E. M. (1995). *Diffusion of Innovations* (4 ed.). New York, New York: The Free Press.
- Rogers, E. M. (2003). *Diffusion of Innovations* (5 ed.). New York, New York: The Free Press.
- Rogers, E. M., & Shoemaker, F. F. (1971). *Communication of Innovations: a Cross-Cultural Approach* (2 ed.). New York, New York: The Free Press.
- Ryan, B., & Gross, N. C. (1943). The Diffusion of Hybrid Seed Corn in Two Iowa Communities. *Rural Sociology*, 8, 15-24.
- Rysavy, P. (2004, October, 14). Wide Area Wireless Data: Forever Evolving. *Network Computing*, 15, 40-46.
- Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived Security and World Wide Web Purchase Intention. *Industrial Management & Data Systems*, 101(3/4), 165-176.
- Sanderson, E., & Forcht, K. A. (1996). Information Security in Business Environments. *Information Management & Computer Security*, 4(1), 32-37.
- Schmidt, M. B., & Arnett, K. P. (2005). Spyware: A Little Knowledge is a Wonderful Thing. *Communications of the ACM*, 48(8).
- Schmidt, M. B., Johnston, A. C., & Arnett, K. P. (2004, August ). *Wireless Network Security in Hospitality SMEs*. Paper presented at the Americas Conference on Information Systems (AMCIS), New York, NY.
- Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems*, 17(4), 5-36.
- Security Efforts Still Lacking. (2003). *Information Management Journal*, 37(1), 15.
- Segars, A. H., & Grover, V. (1998). Strategic Information Systems Planning Success: An Investigation of the Construct and its Measurement. *MIS Quarterly*, 22(2), 139-164.
- Sharma, S. (1996). *Applied Multivariate Techniques*. New York, NY: John Wiley & Sons, Inc.

- Sharma, V. (2004). Intrusion Detection in Infrastructure Wireless LANs. *Bell Labs Technical Journal*, 8(4), 115-119.
- Shim, J. P. (2005). Korea's Lead in Mobile Cellular and DMB Phone Services. *Communications of the Association for Information Systems*, 15, 555-566.
- Shim, J. P., Varshney, U., Dekleva, S., & Knoerzer, G. (2006). Mobile and Wireless Networks: Services, Evolution & Issues. *International Journal of Mobile Communications*, 4(4), 405-417.
- Shim, J. P., Varshney, U., Dekleva, S. M., & Knoerzer, G. (2003). *Mobile Wireless Technology and Services: Evolution and Outlook*. Paper presented at the Ninth Americas Conference on Information Systems (AMCIS), Tampa, FL.
- Shinn, S. (2005, January / February). Knights in Cyber Armor. *BizEd Technology and Security (Published by AACSB International)*, 4, 24-29.
- Signs of the Times. (2005, May / June). *BizEd Technology and Security (Published by AACSB International)*, 4, 52-53.
- Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, 8(1), 31-41.
- Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the Determinants of Risk Behavior. *Academy of Management Review*, 17(1), 9-38.
- Sitkin, S. B., & Weingart, L. K. (1995). Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions. *Academy of Management Journal*, 38 (6), 1573-1592.
- Stair, R. M., & Reynolds, G. W. (2001). *Principles of Information Systems* (5 ed.). Boston: Course Technology Thomson Learning.
- Storey, V. C., Straub, D. W., Stewart, K. A., & Welke, R. J. (2000). A Conceptual Investigation of the E-commerce Industry. *Communications of the ACM*, 43(7), 117-123.
- Straub, D., Boudreau, M.-C., & Gefen, D. (2001). Validation Guidelines for IS Positivist Research. *Communications of AIS*, 13, 2-79.
- Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly*, 13(2), 146-169.

- Straub, D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly*, 14(1), 44-59.
- Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), 441-469.
- Taylor, G. S., & Shim, J. P. (1993). A Comparative Examination of Attitudes Toward Software Piracy Among Professors and Executives. *Human Relations*, 46(4), 419-434.
- Templeton, G. F., & Byrd, T. A. (2003). Determinants of the Relative Advantage of a Structured SDM During the Adoption Stage of Implementation. *Information Technology and Management*, 4(4), 409-428.
- Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (1995, December). *Innovation Diffusion Theory as a Predictor of Adoption Intention for Financial EDI*. Paper presented at the International Conference on Information Systems (ICIS), Amsterdam, Netherlands.
- Torkzadeh, G., & Dhillon, G. (2002). Measuring Factors that Influence the Success of Internet Commerce. *Information Systems Research*, 13(2), 187-204.
- Trauth, E. M. (2001). The Choice of Qualitative Methods in IS Research. In E. M. Trauth (Ed.), *Qualitative Research in IS: Issues and Trends* (pp. 1-19). Hershey, PA: Idea Group Publishing.
- Turban, E., Rainer, R. K., & Potter, R. E. (2002). *Introduction to Information Technology* (2 ed.). Somerset, NJ: Wiley.
- University of Notre Dame. (2005). Indicators of Excellence. Retrieved April, 21, 2005, from <http://und.collegesports.com/school-bio/nd-excellence.html>
- Vaughn, R. B. (2003). Advances in the Provision of System and Software Security -- Thirty Years of Progress. In *Advances in Computers* (Vol. 58): Elsevier.
- Veiga, A. (2004). Best Western to Offer Free High-Speed Internet. Retrieved January 24, 2004, from <http://www.suntimes.com/output/business/bestwestern25.html>
- Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2), 186-207.

- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-478.
- Volonino, L., Gessner, G. H., & Kermis, G. F. (2004). Holistic Compliance with Sarbanes-Oxley. *Communications of AIS*, 2004(14), 219-233.
- Warkentin, M., & Schmidt, M. B. (2003). *Evaluating Executive Perceptions of IS Security Threats and Responses: A Post 9/11 Critique*. Paper presented at the IS OneWorld International Conference, Las Vegas, NV.
- Welch, D., & Lathrop, S. (2003). *Wireless Security Threat Taxonomy*. Paper presented at the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.
- Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, 46(8), 91-95.
- Wingfield, N. (1995, November 16). IS and the 'net. *InfoWorld*, 17, 61-62.
- Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59, 329-349.
- Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communications*, 1(4), 317-342.
- WLAN Security: How Big a Problem? (2004, November). *Business Communications Review*, 34, 6.
- Writing@CSU: Writing Guide. (2004). Retrieved August 24, 2004, from <http://writing.colostate.edu/references/research/glossary/>
- Wynn, E. (2001). Mobius Transitions in the Dilemma of Legitimacy. In E. M. Trauth (Ed.), *Qualitative Research in IS: Issues and Trends*. Hershey, PA: Idea Group Publishing.
- Yin, R. K. (2003). *Case Study Research: Design and Methods* (3 ed.). Thousand Oaks, CA: Sage Publications.
- Yourdon, E. (2002). *Byte Wars: The Impact of September 11 on Information Technology*. Upper Saddle River, NJ: Prentice Hall.



Zmud, R. W. (1984). An Examination of 'Push-Pull' Theory Applied to Process Innovation in Knowledge Work. *Management Science*, 30(6), 727-738.

APPENDIX A  
SURVEY INSTRUMENT

Script to be read to students:

We appreciate your participation. This study is completely anonymous. Your identity will not be traced through your name, identification number, or any other mechanisms. You can quit the survey at any point. Please answer the questions in the most accurate manner possible. Completing the questions will take about 10 minutes.

Our Institutional Review Board (IRB) at Mississippi State University has reviewed and approved this study under number 05-015. If you have any questions, you can reach Dr. Kirk Arnett at (662) 325-1999, Mark Schmidt at (662) 325-3240 or IRB at (662) 325-3994.

Federal guidelines require us to obtain your informed consent for participation in the study. Completing the survey and handing it back to us will be considered your informed consent and your voluntary agreement to participate.

**Part I:** Please circle your answer for each question.

1. What is your age? 18-20, 21-23, 24-26, 27-29, 30-32, >32
2. What is your gender? Female / Male
3. What is your major? Accounting, BIS, Econ, Finance, Management, Marketing  
Other- please list \_\_\_\_\_
4. What is your classification? Freshman, Sophomore, Junior, Senior, Graduate Student,  
Unclassified, Other
5. How many years have you used computers? 0-5, 6-10, 11-15, if greater than 15 please list  
\_\_\_\_\_
6. How many years have you used the wireless data network? Not at all, 1, 2, 3, 4, 5, if > than 5  
please list \_\_\_\_\_
7. How many BIS, CS, or computer related classes have you taken? 0, 1, 2, 3, 4, 5, 6, 7, if > than 7  
please list \_\_\_\_\_
8. Do you have a personal computer (desktop)? Yes / No  
If yes – does it have wireless capabilities? Yes / No
9. Do you have a personal computer (laptop)? Yes / No  
If yes – does it have wireless capabilities? Yes / No
10. Do you have any other form of device with wireless data capabilities (PDA, cell phone etc.)? Yes /  
No
11. Do you use online banking?  
Yes / No
12. How many credit cards do you have? \_\_\_\_\_
13. How many bank accounts do you have? \_\_\_\_\_
14. Do you have a brokerage account(s)?  
Yes / No If yes, is it online? Yes / No
15. Do you own a paper shredder?  
Yes / No
16. During the average school week, approximately how many times do you connect to the wireless  
network? 0-5, 6-10, 11-15, 16-20, 21-25, 26-30, > 31
17. During the average school week, approximately how many minutes long is your average  
connection to the wireless network? 0-20, 21-40, 41-60, 61-80, 81-100, > 100

**Part II:** For each item, please check the response that most accurately reflects your opinion using the following scale:

Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

	Strongly Disagree [1]	[2]	[3]	Neutral [4]	[5]	[6]	Strongly Agree [7]
My professors do not require that I use the wireless network.							
Although it might be helpful, using a wireless network is certainly not compulsory in my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network enables me to accomplish tasks more quickly.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network improves the quality of work I do.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network makes it easier to do my job / school work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network enhances the effectiveness of my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network gives me greater control over my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network is compatible with all aspects of my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I think that using a wireless network fits well with the way I like to work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network fits into my work style.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
People in my organization who use a wireless network have more prestige than those who do not.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
People in my organization who use a wireless network have a high profile.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network is a status symbol in my organization.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
My interaction with a wireless network is clear and understandable.	[1]	[2]	[3]	[4]	[5]	[6]	[7]

I believe that it is easy to get a wireless network to do what I want it to do.	Strongly Disagree	Neutral				Strongly Agree	
	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Overall, I believe that a wireless network is easy to use.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Learning to operate a wireless network is easy for me.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I would have no difficulty telling others about the results of using a wireless network.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe I could communicate to others the consequences of using a wireless network.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
The results of using a wireless network are apparent to me.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I would have difficulty explaining why using a wireless network may or may not be beneficial.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
In my organization, one sees wireless networks being used by many others.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Wireless network use is not very visible in my organization.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Before deciding whether to use any wireless network applications, I was able to properly try them out.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I was permitted to use a wireless network on a trial basis long enough to see what it could do.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe that the security threat of using wireless data technologies is severe.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe that security threat of using wireless data technologies is serious.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe that security threat of using wireless data technologies is significant.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
If I use the wireless network, I am at risk of having my personal data fall into the wrong hands.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
If I use the wireless network, it is likely that I will suffer negative consequences.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
If I use the wireless network, it is possible that I will suffer negative consequences.	[1]	[2]	[3]	[4]	[5]	[6]	[7]

**Part III:**

Please read the following scenario and answer the questions:

Congratulations! You have won one million dollars. After taxes you are left with \$600,000 (of course Uncle Sam gets some of your money – get used to it)! You have decided to invest your \$600,000 in the stock market. As you may know, the stock market can be very volatile. For example, recently Enron lost over half its value in less than one day. If you own stock that goes down, you will lose money.

Obviously you want to maximize your wealth so you can retire early. To that end, you want to monitor your stock investments with your online broker. You have access to a computer at your home (this computer is connected to the Internet via a wired connection). However, much of the day you are away at school and do not have access to a wired network (because the labs are closed for upgrades). Fortunately, you have access to a wireless network while at school.

You are relatively sure that your username and password and hence your \$600,000 investment is secure when you log on to your account. However, as security issues have been raised about both networks, there is a chance that computer criminals could intercept your personal information.

Your dilemma is then:

- You want to monitor your investment frequently throughout the day so you don't miss out on the opportunity to unload a stock whose price is dropping rapidly.
- You have the opportunity to monitor your investment on the wireless network while you are at school – but you may have concerns about the security of your information. The computer criminals are not perfect – if you check your stocks once a day they are not likely to get your personal information. But you may learn about events too late and lose money. But if you check every 5 minutes the chances of having your information intercepted increases.

Please answer the following questions:

If you wanted to check your account frequently how many times a day would you use the convenient but possibly risky wireless network?

\_\_\_ Never

\_\_\_ 1-5

\_\_\_ 6-10

\_\_\_ 11-15

\_\_\_ 16-20

\_\_\_ 21 or more

Please describe why you answered the way you did:

On a scale from 1 to 10, how concerned would you be regarding security? (1 is low – 10 is high)

1 2 3 4 5 6 7 8 9 10

Please tell us anything else that you feel important about the use and security of wireless networks on your college campus:

Please tell us anything else that you feel important about the use and security of wireless networks at your residence:

Please tell us anything else that you feel important about the use and security of wireless networks in business:

All factors considered, which do you prefer to use a (circle one) wired or wireless network?

Please describe why:

What (if any) steps do you take to reduce security threats while you are using the wireless network?

Are there activities that you would do on a wired network but would not do on a wireless network because of security concerns? If yes, please describe.

Your answers to these questions are very important for our research on the security of wireless networks.

We appreciate your assistance!



APPENDIX B  
STRUCTURED INTERVIEW QUESTIONS

Name: \_\_\_\_\_ Title \_\_\_\_\_

1. What is the nature of your position?
2. Do you think students adopt wireless technologies?
3. Why or why not?
4. What factors led to the decision to implement wireless technologies on the campus?
5. What is the primary purpose of the wireless network on campus?
6. What are the advantages of the wireless network compared to the traditional network technologies available on campus?
7. How easy to use is the wireless network for students?
8. Do you believe the use of the wireless network to be associated with a student's perception of image or status?
9. What are the issues regarding wireless network availability and compatibility?
10. What measures do you take to secure the wireless network?
11. Do you consider the wireless network secure?
12. Has anyone ever broken into the wireless network?

13. What wireless standard do you use for your wireless network? 802.11B or G?
14. What security mechanisms are employed to defend the network?
15. Are there any other mechanisms that could be deployed?
16. What (if any) steps do you take to reduce security threats while you are using the wireless network?
17. Do you feel that your organization is better prepared than other organizations to handle security issues with wireless? Please explain.
18. Do you plan on taking any additional steps as a result of this meeting?
19. Is there anything else you like to share with me today?

Please look at the following taxonomy (list) of risks. Considering the threat categories, the given examples, and your own examples of threats, please characterize your wireless network's level of vulnerability to the each category. Which of these gives you the most concern? Why?

- I. Internal
  - a. Human
    - i. Deliberate
      1. Unauthorized access by employees
      2. Employees intentionally entering improper data
      3. Intentional destruction of data by employees
      4. Theft of hardware, software, data, or information
    - ii. Unintentional
      1. Data entry error by employees
      2. Accidental destruction of data by employees
      3. Improper media handling
  - b. Nonhuman
    - i. Deliberate
    - ii. Unintentional
      1. Weak / ineffective controls
      2. Inadequate control over media
      3. Poor control of input / output
- II. External
  - a. Human
    - i. Deliberate
      1. Hackers / crackers
      2. Access to system by competitors
      3. Social engineering
      4. Dumpster diving
      5. Cyber terrorism
      6. Web site vandalism
      7. Theft of hardware, software, data, or information
    - ii. Unintentional
  - b. Nonhuman
    - i. Deliberate
      1. Viruses / worms / Trojan horses
      2. Denial of service attacks
    - ii. Unintentional
      1. Natural disasters (fires, earthquakes, hurricanes, tornados, floods, storms, severe snow...)
      2. Blackouts / brownouts

Considering the preceding list of threats as well as your own list of threats, how well is your organization prepared to deal with these threats?

Not prepared  
1      2      3      4      5      6      7      8      9      10  
Very prepared

Please elaborate:

Considering the preceding list of threats as well as your own list of threats, how well are other organizations similar to yours prepared to deal with these threats?

Not prepared  
1      2      3      4      5      6      7      8      9      10  
Very prepared

Please elaborate:

Part I: Please circle your answer for each question (answer as a decision maker).

1. What is your age? 18-20, 21-23, 24-26, 27-29, 30-32, >32
2. What is your gender? Female / Male
3. What is your major? Accounting, BIS, Econ, Finance, Management, Marketing  
Other- please list \_\_\_\_\_
4. What is your classification? Freshman, Sophomore, Junior, Senior, Graduate Student,  
Unclassified, Other
5. How many years have you used computers? 0-5, 6-10, 11-15, if greater than 15 please list  
\_\_\_\_\_
6. How many years have you used the wireless data network? Not at all, 1, 2, 3, 4, 5, if > than 5  
please list \_\_\_\_\_
7. How many BIS, CS, or computer related classes have you taken? 0, 1, 2, 3, 4, 5, 6, 7, if > than 7  
please list \_\_\_\_\_
8. Do you have a personal computer (desktop)? Yes / No  
If yes – does it have wireless capabilities? Yes / No
9. Do you have a personal computer (laptop)? Yes / No  
If yes – does it have wireless capabilities? Yes / No
10. Do you have any other form of device with wireless data capabilities (PDA, cell phone etc.)? Yes /  
No
11. Do you use online banking?  
Yes / No
12. How many credit cards do you have? \_\_\_\_\_
13. How many bank accounts do you have? \_\_\_\_\_
14. Do you have a brokerage account(s)?  
Yes / No If yes, is it online? Yes / No
15. Do you own a paper shredder?  
Yes / No
16. During the average school week, approximately how many times do you connect to the wireless  
network? 0-5, 6-10, 11-15, 16-20, 21-25, 26-30, > 31
17. During the average school week, approximately how many minutes long is your average  
connection to the wireless network? 0-20, 21-40, 41-60, 61-80, 81-100, > 100

**Part II:** For each item, please check the response that most accurately reflects your opinion using the following scale:

Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

	Strongly Disagree [1]	[2]	[3]	Neutral [4]	[5]	[6]	Strongly Agree [7]
My professors do not require that I use the wireless network.							
Although it might be helpful, using a wireless network is certainly not compulsory in my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network enables me to accomplish tasks more quickly.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network improves the quality of work I do.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network makes it easier to do my job / school work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network enhances the effectiveness of my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network gives me greater control over my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network is compatible with all aspects of my work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I think that using a wireless network fits well with the way I like to work.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network fits into my work style.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
People in my organization who use a wireless network have more prestige than those who do not.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
People in my organization who use a wireless network have a high profile.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Using a wireless network is a status symbol in my organization.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
My interaction with a wireless network is clear and understandable.	[1]	[2]	[3]	[4]	[5]	[6]	[7]

I believe that it is easy to get a wireless network to do what I want it to do.	Strongly Disagree	Neutral				Strongly Agree	
	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Overall, I believe that a wireless network is easy to use.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Learning to operate a wireless network is easy for me.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I would have no difficulty telling others about the results of using a wireless network.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe I could communicate to others the consequences of using a wireless network.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
The results of using a wireless network are apparent to me.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I would have difficulty explaining why using a wireless network may or may not be beneficial.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
In my organization, one sees wireless networks being used by many others.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Wireless network use is not very visible in my organization.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Before deciding whether to use any wireless network applications, I was able to properly try them out.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I was permitted to use a wireless network on a trial basis long enough to see what it could do.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe that the security threat of using wireless data technologies is severe.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe that security threat of using wireless data technologies is serious.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
I believe that security threat of using wireless data technologies is significant.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
If I use the wireless network, I am at risk of having my personal data fall into the wrong hands.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
If I use the wireless network, it is likely that I will suffer negative consequences.	[1]	[2]	[3]	[4]	[5]	[6]	[7]
If I use the wireless network, it is possible that I will suffer negative consequences.	[1]	[2]	[3]	[4]	[5]	[6]	[7]



**Part III:**

Please read the following scenario and answer the questions:

Congratulations! You have won one million dollars. After taxes you are left with \$600,000 (of course Uncle Sam gets some of your money – get used to it)! You have decided to invest your \$600,000 in the stock market. As you may know, the stock market can be very volatile. For example, recently Enron lost over half its value in less than one day. If you own stock that goes down, you will lose money.

Obviously you want to maximize your wealth so you can retire early. To that end, you want to monitor your stock investments with your online broker. You have access to a computer at your home (this computer is connected to the Internet via a wired connection). However, much of the day you are away at school and do not have access to a wired network (because the labs are closed for upgrades). Fortunately, you have access to a wireless network while at school.

You are relatively sure that your username and password and hence your \$600,000 investment is secure when you log on to your account. However, as security issues have been raised about both networks, there is a chance that computer criminals could intercept your personal information.

Your dilemma is then:

- You want to monitor your investment frequently throughout the day so you don't miss out on the opportunity to unload a stock whose price is dropping rapidly.
- You have the opportunity to monitor your investment on the wireless network while you are at school – but you may have concerns about the security of your information. The computer criminals are not perfect – if you check your stocks once a day they are not likely to get your personal information. But you may learn about events too late and lose money. But if you check every 5 minutes the chances of having your information intercepted increases.

Please answer the following questions:

If you wanted to check your account frequently how many times a day would you use the convenient but possibly risky wireless network?

\_\_\_ Never

\_\_\_ 1-5

\_\_\_ 6-10

\_\_\_ 11-15

\_\_\_ 15-20

\_\_\_ 21 or more

Please describe why you answered the way you did:

On a scale from 1 to 10, how concerned would you be regarding security? (1 is low – 10 is high)

1 2 3 4 5 6 7 8 9 10

Please tell us anything else that you feel important about the use and security of wireless networks on your college campus:

Please tell us anything else that you feel important about the use and security of wireless networks at your residence:

Please tell us anything else that you feel important about the use and security of wireless networks in business:

All factors considered, which do you prefer to use a (circle one) wired or wireless network?

Please describe why:

What (if any) steps do you take to reduce security threats while you are using the wireless network?

Are there activities that you would do on a wired network but would not do on a wireless network because of security concerns? If yes, please describe.

Your answers to these questions are very important for our research on the security of wireless networks.

We appreciate your assistance!

## APPENDIX C

### THE ORIGINAL PCI AND THREAT ITEMS

The following questions will be answered using the following Likert Scale:

Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
----------------------	----------	----------------------	---------	-------------------	-------	-------------------

\* Questions preceded with an \* reflect items recommended by Moore and Benbasat for inclusion in the “short” scale. The final instrument will just include these 25 items combined with the six items from Witte et al. for a total of 31 items.

#### Voluntariness

1. My professors expect me to use the wireless network.
2. My use of the wireless network is voluntary (as opposed to required by professors or others).
3. My professors do not require that I use the wireless network.
4. Although it might be helpful, using a wireless network is certainly not compulsory in my work.

#### Relative Advantage

1. Using a wireless network enables me to accomplish tasks more quickly.
2. Using a wireless network improves the quality of work I do.
3. Using a wireless network makes it easier to do my job / school work.
4. The disadvantages of me using a wireless network far outweigh the advantages.
5. Using a wireless network improves my school performance.
6. Overall, I find using a wireless network to be advantageous to my work.
7. Using a wireless network enhances the effectiveness of my work.
8. Using a wireless network gives me greater control over my work.
9. Using a wireless network increases my productivity.

### Compatibility

1. Using a wireless network is compatible with all aspects of my work.
2. Using a wireless network is completely compatible with my current situation.
3. I think that using a wireless network fits well with the way I like to work.
4. Using a wireless network fits into my work style.

### Image

1. Using a wireless network improves my image with the organization.
2. Because of my use of a wireless network, others in my organization see me as more valuable.
3. People in my organization who use a wireless network have more prestige than those who do not.
4. People in my organization who use a wireless network have a high profile.
5. Using a wireless network is a status symbol in my organization.

### Ease of use

1. I believe that a wireless network is cumbersome to use.
2. It is easy for me to remember how to perform tasks using a wireless network.
3. My using a wireless network requires a lot of mental effort.
4. Using a wireless network is often frustrating.
5. My interaction with a wireless network is clear and understandable.
6. I believe that it is easy to get a wireless network to do what I want it to do.
7. Overall, I believe that a wireless network is easy to use.
8. Learning to operate a wireless network is easy for me.

### Result Demonstrability

1. I would have no difficulty telling others about the results of using a wireless network.
2. I believe I could communicate to others the consequences of using a wireless network.
3. The results of using a wireless network are apparent to me.
4. I would have difficulty explaining why using a wireless network may or may not be beneficial.

### Visibility

1. I have seen what others do using a wireless network.
2. In my organization, one sees wireless networks being used by many others.
3. I have seen a wireless network in use outside my organization.
4. Wireless network use is not very visible in my organization.
5. It is easy for me to observe others using wireless network in my firm.
6. I have had plenty of opportunity to see the wireless network being used.
7. I have not seen many others using a wireless network in my department.

### Trialability

1. I've had a great deal of opportunity to try various wireless network applications.
2. I know where I can go to satisfactorily try out various uses of a wireless network.
3. A wireless network was available to me to adequately test run various applications.

4. Before deciding whether to use any wireless network applications, I was able to properly try them out.
5. I was permitted to use a wireless network on a trial basis long enough to see what it could do.
6. I am able to experiment with the wireless network as necessary.
7. I can have wireless network applications for long enough periods to try them out.
8. I did not have to expend very much effort to try out the wireless network.
9. I don't really have adequate opportunities to try out different things on the wireless network.
10. A proper on-the-job tryout of the various uses of the wireless network is not possible.
11. There are enough people in my organization to help me try the various use of the wireless network.

Note: the following two constructs will be measured by the full set of items.

#### Severity of Threat

1. I believe that the security threat of using wireless data technologies is severe.
2. I believe that security threat of using wireless data technologies is serious.
3. I believe that security threat of using wireless data technologies is significant.

#### Susceptibility to Threat

1. If I use the wireless network, I am at risk of having my personal data fall into the wrong hands.
2. If I use the wireless network, it is likely that I will suffer negative consequences.
3. If I use the wireless network, it is possible that I will suffer negative consequences.

APPENDIX D

CONSTRUCTS, ITEMS, AND CORRESPONDING

QUESTIONS



Table D.1

## Constructs, Items, and Corresponding Questions

Construct	Item	Question
Improvement Potential	Wquickly	Using a wireless network enables me to accomplish tasks more quickly.
	ImprovQual	Using a wireless network improves the quality of work I do.
	Ejob	Using a wireless network makes it easier to do my job / school work.
	Effective	Using a wireless network enhances the effectiveness of my work.
	Control	Using a wireless network gives me greater control over my work.
	Compatible	Using a wireless network is compatible with all aspects of my work.
	FitsWork	I think that using a wireless network fits well with the way I like to work.
	FitsStyle	Using a wireless network fits into my work style.
Usage	Clear	My interaction with a wireless network is clear and understandable.
	EasyToGet	I believe that it is easy to get a wireless network to do what I want it to do.
	EasyToUse	Overall, I believe that a wireless network is easy to use.
	EasyOperate	Learning to operate a wireless network is easy for me.

Table D.1 continued

Construct	Item	Question
Usage	TellOthers	I would have no difficulty telling others about the results of using a wireless network.
	CommConsequ	I believe I could communicate to others the consequences of using a wireless network.
	ApparentResults	The results of using a wireless network are apparent to me.
	DiffExplainBene	I would have difficulty explaining why using a wireless network may or may not be beneficial.
Susceptibility and Severity of Threat	SecuritySevere	I believe that the security threat of using wireless data technologies is severe.
	SecuritySerious	I believe that security threat of using wireless data technologies is serious.
	SecuritySignificant	I believe that the security threat of using wireless data technologies is significant.
	DataWrongHands	If I use the wireless network, I am at risk of having my personal data fall into the wrong hands.
	NegConLikely	If I use the wireless network, it is likely that I will suffer negative consequences.
	NegConPoss	If I use the wireless network, it is possible that I will suffer negative consequences.

Table D.1 continued

Construct	Item	Question
Image	Prestige	People in my organization who use a wireless network have more prestige than those who do not.
	Profile	People in my organization who use a wireless network have a high profile.
	Status	Using a wireless network is a status symbol in my organization.
Voluntariness	ProfRequire	My professors do not require that I use the wireless network.
	NotCompuls	Although it might be helpful, using a wireless network is certainly not compulsory in my work.
Visibility	SeeOthers	In my organization, one sees wireless networks being used by many others.
	NotVisable	Wireless network use is not very visible in my organization.
Triability	ProperlyTry	Before deciding whether to use any wireless network applications, I was able to properly try them out.
	PermittedToUse	I was permitted to use a wireless network on a trial basis long enough to see what it could do.